

Der Bundesrat

19. Juni 2024

Beeinflussungsaktivitäten und Desinformation

Bericht des Bundesrates in Erfüllung des Postulats 22.3006 SiK-N

Inhalt

1. Einleitung

1.1 Postulat 22.3006

Im Januar 2022 reichte die Sicherheitspolitische Kommission des Nationalrats (SiK-N) ein Postulat ein, welches eine Auslegeordnung zur Bedrohung der Schweiz durch Desinformationskampagnen verlangt.

Konkret soll der Bundesrat in einem Bericht darlegen, inwiefern die Schweiz von Beeinflussungsaktivitäten bzw. Desinformationskampagnen betroffen ist. Des Weiteren sind Massnahmen vorzuschlagen, wie der Bedrohung zu begegnen ist. Das Postulat beruft sich dabei auf den Sicherheitspolitischen Bericht 2021 des Bundesrats, welcher das Thema vertiefte und darlegte, dass Beeinflussungsaktivitäten politische Prozesse sabotieren sowie das Vertrauen der Bevölkerung in Institutionen untergraben können. Angesichts der machtpolitischen Konfrontationen wächst auch für die Schweiz das Risiko, von solchen Aktivitäten betroffen zu sein.

Der Bundesrat beantragte am 23. Februar 2022 die Annahme des Postulates. Der Nationalrat nahm das Postulat am 9. März 2022 an.

1.2 Aktualität und Einordnung

Die Sicherheitslage in Europa und im Umfeld der Schweiz ist instabiler, unübersichtlicher und unberechenbarer geworden. Spannungen und Rivalitäten zwischen den Grossmächten haben zugenommen. Mit Russlands militärischer Aggression gegen die Ukraine ist Krieg zurück in Europa und die Sicherheitsordnung des Kontinents nachhaltig erschüttert. Alte und neue bewaffnete Konflikte rund um Europa sind aufgeflammt. Im Nahen Osten etwa drohen diese weiter zu eskalieren, mit globalen Auswirkungen. Viele Gesellschaften in westlichen Ländern sind zunehmend polarisiert. Demokratische Werte und völkerrechtliche Normen sind weltweit unter Druck. Die Art, wie Konflikte ausgetragen werden, wandelt sich, geprägt von machtpolitischen und technologischen Veränderungen. Der Informationsraum spielt eine wichtige Rolle in Konflikten, wie man etwa im Krieg gegen die Ukraine oder rund um den Krieg zwischen Israel und der Hamas sieht, und ist Raum für Beeinflussungsaktivitäten verschiedener Staaten.

Der Einsatz von Mitteln, die zum Repertoire hybrider Konfliktführung zählen, wie etwa Cyberangriffe und Beeinflussungsaktivitäten, hat sich seit dem Sicherheitspolitischen Bericht 2021 verstärkt. Staaten, welche die bestehenden Machtverhältnisse mit Gewalt verteidigen oder verändern wollen, agieren mehr als früher in der Grauzone zwischen bewaffnetem Konflikt und Frieden. Der Einsatz von Mitteln hybrider Konfliktführung ist oft vielschichtig und unberechenbar. Akteure, welche solche Mittel anwenden, können ihre Urheberschaft oftmals plausibel abstreiten. Offene, demokratische Gesellschaften können lohnende Ziele sein, um auf deren freie Debatten und demokratische Prozesse Einfluss zu nehmen. Dies kann eine Bedrohung für die innere oder die äussere Sicherheit darstellen. Entsprechend sollen Beeinflussungsversuchen durch staatliche oder staatlich beauftragte Stellen besser erkannt und ihnen begegnet werden.

Beeinflussungsaktivitäten im Informationsraum allgemein, zu denen Desinformation gehört (siehe 2.1 für Begriffe), werden in vielen westlichen Staaten in Politik und Medien intensiv diskutiert. Oftmals wird ihnen sehr grosses destruktives Potenzial zugeschrieben. Sie sind indes keine neue Herausforderung, werden heute aber nicht nur durch die machtpolitischen Verschiebungen, sondern auch durch die technologischen Möglichkeiten, die Geschwindigkeit der Informationsverbreitung und die zunehmende Rolle von Unternehmen – von Social-Media-Plattformen bis «Trollfarmen» – bei der Erzeugung und Verbreitung von Desinformation verschärft. Die verbreitete Nutzung von sozialen Medien und die zunehmenden Möglichkeiten, mittels künstlicher Intelligenz (KI) Bild-, Audio- oder Videomaterial zu generieren und zu verbreiten, verschärfen die Herausforderung. Beeinflussungsaktivitäten können zudem von Cyberangriffen begleitet und begünstigt sein. Die wachsende gesellschaftliche Polarisierung ist zugleich Nährboden und Ziel der Beeinflussungsaktivitäten.

Vor allem staatliche und staatlich beauftragte Akteure wenden Mittel und Methoden der Beeinflussung und Desinformation an und betreiben diese oftmals umfassend, koordiniert und mit erheblichen Ressourcen. Aus Schweizer Sicht und staats- und sicherheitspolitisch besonders relevant sind Akteure, welche offensiv andere Werte, Normen und politische Systeme vertreten und demokratische Institutionen untergraben wollen. Die Aktivitäten Russlands, aber auch Chinas, dürften mittel- und langfristig die grösste Relevanz für die Sicherheit der Schweiz behalten.

Auch westliche Staaten und Bündnisse sind im Informationsraum aktiv und versuchen, in politischen Diskussionen in anderen Ländern ihre Sicht einzubringen. Sie sind jedoch für die Schweiz sicherheitspolitisch nicht als Bedrohung einzustufen, wenn sie nicht die staatliche Ordnung der Schweiz und das Funktionieren demokratischer Staatssysteme in Frage stellen oder untergraben.

Aktuelle Beispiele von Beeinflussungsaktivitäten im Informationsraum kann rund um den Krieg in der Ukraine beobachten. Einem globalen Publikum bieten russische Kanäle in sozialen und Online-Medien eine alternative Interpretation, Desinformation und die gezielte Verfälschung der Realität in der Ukraine. Der Kreml kontrolliert indes seinerseits erfolgreich den Informationsfluss in Russland sowie in den besetzten ukrainischen Gebieten durch repressive Massnahmen. Auch Chinas Beeinflussungsaktivitäten weltweit und insbesondere in den westlichen Staaten werden zahlreicher. Sie sind systemisch und strategisch, da viele entsprechende Aktivitäten auf Anregung und unter der Leitung der Kommunistischen Partei Chinas durchgeführt werden. Sie dienen politischen und ideologischen Interessen, die weitgehend breit akzeptierten demokratischen Prinzipien widersprechen. Gleichzeitig verschärft China seine eigenen Gesetze, um sich gegen ausländische Einflüsse auf dem eigenen Territorium zu schützen. Auch viele andere Staaten verschärfen ihre Vorschriften, um den nationalen Informationsraum besser kontrollieren zu können.

Auch die Schweiz, ihre Gesellschaft und ihre Behörden sind vermehrt von Beeinflussungsaktivitäten betroffen. Ihr Bekenntnis zum Völkerrecht und zur Demokratie und der zunehmende Druck, sich im globalen machtpolitischen Gefüge zu positionieren, sind Faktoren dafür. Als Staat mitten in Europa, als Teil der westlichen Wertegemeinschaft und des westlichen Informationsraums sowie wegen ihrer starken wirtschaftlichen und politischen Vernetzung ist die Schweiz bereits seit Jahren indirekt Ziel von Beeinflussungsaktivitäten, die allgemein auf westliche Staaten abzielen. Solche Aktivitäten zielen aber auch zunehmend direkt auf die Schweiz. Es besteht zudem das Risiko, dass das Territorium der Schweiz als Drehscheibe missbraucht wird, um Beeinflussungsaktivitäten gegen Drittstaaten oder gegen internationale Organisationen durchzuführen oder zu finanzieren.

Die Schweiz ist gefordert, systematische staatliche oder staatlich beauftragte Beeinflussung im Informationsraum zu erkennen, ihre Absicht und Urheberschaft zu ermitteln, und gegebenenfalls darauf zu reagieren. Das Potenzial und die Funktionsweise von Beeinflussungsaktivitäten angemessen einzuschätzen ist dafür zentral.

1.3 Fokus und Aufbau des Berichts

Der vorliegende Bericht fokussiert auf die Betroffenheit der Schweiz von Beeinflussungsaktivitäten, deren Wirkung sich im Informationsraum entfaltet und die primär von staatlichen oder staatlich beauftragten ausländischen Akteuren ausgehen, denn diese ist sicherheitspolitisch besonders relevant. Der Bericht beleuchtet die Auswirkungen der Thematik auf sicherheits- und staatspolitische Aspekte und damit darauf, wie sie sich direkt und indirekt auf die Funktionen, Resilienz und den Zusammenhalt von Staat und Gesellschaft auswirkt.

Der Bericht legt die Begrifflichkeiten dar und beschreibt Ziele, Mechanismen, Akteure und Effekte von Beeinflussungsaktivitäten im Informationsraum einschliesslich Desinformation (Kap. 2). Er beschreibt den Umgang anderer Staaten, Bündnisse und Organisationen mit dem Thema (Kap. 3). Anschliessend legt er die Bedrohungslage, Betroffenheit und spezifischen Charakteristiken der Schweiz dar, einschliesslich Fallbeispiele (Kap. 4), und die derzeitigen rechtlichen Rahmenbedingungen (Kap. 5). Er zeigt die bisherigen Arbeiten und Zuständigkeiten in der Schweiz (Kap. 6) sowie mögliche Handlungsoptionen auf (Kap. 7). Ein Glossar am Ende umfasst die gängigen Begriffe im Zusammenhang mit diesem Thema.

2. Beeinflussungsaktivitäten und Desinformation verstehen

2.1 Definitionen und Begriffe

Sicherheitspolitisch besonders relevant sind Beeinflussungsaktivitäten dann, wenn sie von Staaten ausgehen und sich gegen das Funktionieren eines Staats und einer Gesellschaft richten und darauf abzielen, die demokratische Ordnung eines Staats zu unterminieren. Dies grenzt Beeinflussungsaktivitäten

von üblicher Interessenvertretung z. B. im Rahmen der Diplomatie oder der Politik ab, die auf legitime Art und Weise zu Meinungsbildung beitragen soll. Dieser Bericht fokussiert auf Beeinflussungsaktivitäten im Informationsraum in Abgrenzung etwa zu Cyberangriffen oder Beeinflussungsaktivitäten, die militärische Mittel nutzen, etwa Sabotage oder der Einsatz von Truppen im Ausland ohne staatliche Kennzeichen. Er fokussiert auf sicherheitspolitisch besonders relevante ausländische staatliche oder staatlich beauftragte Akteure; dies etwa in Abgrenzung zu Aktivitäten von terroristischen Gruppen oder von Wirtschafts-Akteuren mit rein monetären Zielen.

Für die Begriffe Beeinflussung und Desinformation bestehen keine allgemein anerkannten präzisen Definitionen. Ein Grundverständnis der Begriffe ist den meisten Arbeiten jedoch gemein. Unter **Beeinflussungsaktivitäten im Informationsraum** sind verschiedene Verhalten und Strategien zu verstehen, welche mit manipulativer Absicht darauf abzielen, die Wahrnehmung, das Denken und das Handeln von Individuen, Gruppen und Gesellschaften zu beeinflussen. Diese Aktivitäten können sowohl von staatlichen oder nichtstaatlichen Akteuren betrieben werden. Neben Desinformation beinhaltet das Instrumentarium auch andere Mittel der Beeinflussung im Informationsraum, etwa das absichtliche Weglassen oder Uminterpretieren von Tatsachen, die Manipulation visueller Inhalte, die Nutzung falscher Profile in den sozialen Medien oder Zensur.

Desinformation beschreibt irreführende oder vollständig erfundene Informationen, die absichtlich verwendet werden, um auf die Meinungsbildung der Bevölkerung Einfluss zu nehmen, politische Prozesse zu beeinflussen, die Glaubwürdigkeit von Institutionen und Medien zu unterminieren oder Zweifel an der Zuverlässigkeit von Informationen zu säen.[1] Die EU und die Nato, die ähnliche Definitionen verwenden, verstehen unter Desinformation im weiteren Sinne Informationen, die nachprüfbar falsch oder irreführend sind und die aus Gewinnstreben oder in der bewussten Absicht, die Öffentlichkeit zu täuschen, erstellt, vorformuliert und verbreitet werden.[2] Desinformation kann von unterschiedlichen Akteuren mit verschiedenen Motiven erstellt und verbreitet werden. Nicht jede Art von Desinformation ist eine Beeinflussungsaktivität oder gar sicherheits- oder staatspolitisch relevant.

Sowohl Beeinflussungsaktivitäten als auch Desinformation sind massgeblich davon geprägt, dass falsche Informationen vorsätzlich verbreitet werden, also mit der Absicht der Täuschung, im Gegensatz etwa zu (gutgläubiger) Falsch- bzw. Fehlinformation (englisch angelehnt: Misinformation; für diesen und weitere Begriffe, siehe Glossar). Desinformation oder Beeinflussungsaktivitäten umfassen damit keine in gutem Glauben gemachten Fehler und verbreiteten Fehlinformationen, keine Satire, Parodie oder eindeutig als solche gekennzeichneten parteiischen Informationen und Kommentare.

2.2 Ziele und Methoden

Von Staaten ausgeübte Beeinflussungsaktivitäten richten sich oft gegen offene und demokratische Gesellschaften, die auf einem redlichen Wettbewerb der Ideen auf einer anerkannten Faktenbasis beruhen und wo die freie Verbreitung von Informationen – auch falschen – ein Grundrecht ist. Das Ziel solcher Aktivitäten im Informationsraum ist in der Regel, die öffentliche Meinung und politische oder andere Entscheidungen zu beeinflussen, um eine bestimmte Sichtweise bei einer Zielgruppe zu verankern und die Glaubwürdigkeit der Gegenpartei zu schwächen. Die Zielbevölkerung soll mittels diesen Beeinflussungsaktivitäten verunsichert, verängstigt, aufgebracht oder gespalten werden. Das Vertrauen in staatliche Institutionen soll unterminiert werden.

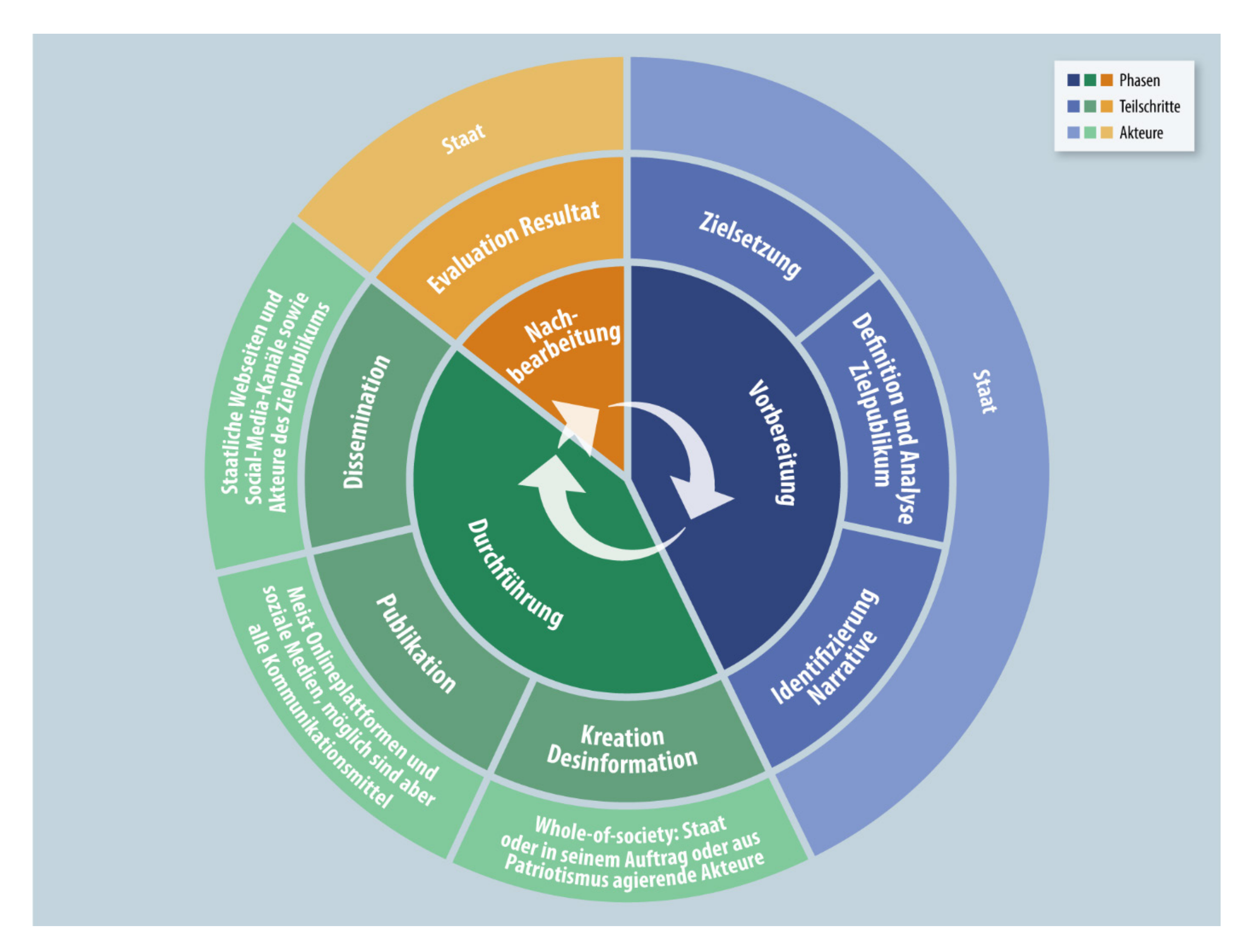
Informationsinhalte werden dabei von einer oder mehreren Quellen über verschiedene Informationskanäle einem Publikum überbracht. Meist definieren Beeinflussungsakteure dieses Publikum zuvor und wählen den Kontext und Zeitpunkt der Informationsaktivitäten zur Erzielung eines grösstmöglichen Effektes. Sie können mehrere Aktivitäten im Rahmen einer Operation koordinieren. Grafik 1 illustriert die Elemente der Vorbereitung einer solchen koordinierten Aktion und die folgenden Schritte. Nicht alle Aktivitäten sind unbedingt von langer Hand oder detailliert geplant; und das intendierte Ziel zu erreichen ist nie garantiert, auch bei genauer Planung und hohem Ressourceneinsatz.

Ein Verständnis von Zielgruppen sind für Beeinflussungsakteure besonders wichtig. Bei Individuen spielen z. B. bestimmte Charaktereigenschaften wie Eitelkeit oder aufrichtige Hilfsbereitschaft und bei Gruppen bestimmte soziodemographische oder kollektive Eigenschaften wie nationale Traumata oder gesell-

[1] Bundesamt für Kommunikation, Bericht "Desinformation in der Schweiz 2021"

[2] Siehe <https://commission.europa.eu> und <https://www.nato.int>.

schaftliche Bruchlinien, die ausgenutzt werden können, eine Rolle. Es ist anzunehmen, dass Autorinnen und Autoren von Beeinflussungsaktivitäten ihr Zielpublikum nicht immer präzise erreichen oder ihren Inhalt präzise tarieren können. Desinformation hat jedoch bereits einen Effekt, wenn Zweifel an etablierten Fakten oder offiziellen Informationen gesät werden, ohne dass der spezifische Desinformationsinhalt als wahr angesehen wird. Es gibt auch Anzeichen dafür, dass Beeinflussungsaktivitäten sich einer Vielzahl verschiedenen und teilweise auch widersprüchlichen Narrative bedienen, um die Erfolgschancen bei unterschiedlichen Zielgruppen zu erhöhen. Beeinflussungsaktivitäten sind riskant und eine Enttarnung der Urheberschaft könnte kontraproduktiv sein, weshalb zu deren Verschleierung meist erheblicher Aufwand betrieben wird.



Grafik 1: Beispielhafter Ablauf und Akteure einer Desinformationsoperation durch einen Staat

Selbst wenn Desinformationen als solche identifiziert und widerlegt wurden, werden sie oftmals weiterhin verbreitet. Es ist in der Psychologie erwiesen, dass oft wiederholten Aussagen eher geglaubt wird, unabhängig von ihrem Wahrheitsgehalt (Scheinwahrheitseffekt).[3]

Beeinflussungsaktivitäten im Informationsraum umfassen ein breites Spektrum von Methoden wie beispielsweise die Manipulation audiovisueller Inhalte, das Herausreissen der Information aus ihrem Kontext, die Entwicklung neuer Narrative und die Verbreitung über nicht-authentische Online-Konten. Methoden zielen in der Regel darauf ab, dass Desinformation für das jeweilige Zielpublikum nur schwer von akkurater, ausgewogener Berichterstattung zu unterscheiden ist. Informationsinhalte werden deshalb auch in seriös und objektiv wirkenden Medien oder alternativen Onlinemedien aufgenommen. Begünstigt

[3] Catherine Hackett Renner, *Validity effect,* in: Rüdiger F. Pohl (Hrsg.), “*Cognitive illusions”,* Psychology Press (Hove, UK: 2004), S. 201–213.

wird die Glaubwürdigkeit von Desinformation, wenn sie sich auf Aussagen angeblicher Expertinnen oder Experten stützt.

Eine Methode ist auch, bekannte Medienportale visuell zu klonen, mit Desinformation zu füllen und so von der Glaubwürdigkeit und Popularität dieser Medien zu profitieren. Recherchen der deutschen Presse und der NGOs DisinfoLab und Qurium deckten Ende 2022 die Operation «Doppelgänger» auf. Diese produzierte mehr als 60 gefälschte Nachrichtenseiten, die grosse internationale Medien (Le Monde, The Guardian, Spiegel usw.) imitierten, aber auch über 1600 Konten und mehrere hundert gefälschte Seiten in sozialen Netzwerken. Laut dem Sicherheitsbericht von Meta vom 29. August 2023 diente die Operation dazu, Desinformation im Sinne Russlands über den Krieg gegen die Ukraine zu verbreiten.[4]

Des Weiteren können Cyberangriffe Beeinflussungsaktivitäten zudienen, etwa zum Diebstahl von sensiblen bzw. klassifizierten Informationen, welche später in originaler oder manipulierter Form im Rahmen einer Beeinflussungsaktivität einem Zielpublikum zugeführt werden («*hack and leak*»).

2.3 Akteure

Beeinflussungsaktivitäten umfassen viele mögliche Akteure, wie Grafik 1 illustriert, darunter staatliche Stellen, Unternehmen wie Plattformen oder Medienunternehmen, und Einzelpersonen wie Mediennutzerinnen und -nutzer; wissentlich und evt. beauftragt, oder unwissentlich. Dies macht die Koordination und Kontrolle über den Prozess für Beeinflussungsakteure schwierig und trägt auch dazu bei, dass entsprechende Aktivitäten auch bei grossem Mitteleinsatz nicht automatisch erfolgreich sind.

Politische und echte oder scheinbar echte zivilgesellschaftliche Akteure können Vehikel von Beeinflussungsaktivitäten sein. Zur Verbreiterung seiner Sicht nutzt z. B. Russland oft betont apolitische Tarninstitutionen und -vereine als Fassade sowie gewisse russlandfreundliche Parteien und Politiker in westlichen Staaten. Die Verbindung zum oder Finanzierung durch den russischen Staat muss für diese Beteiligten nicht offensichtlich sein. Der Kreml schuf mittels Parteispenden, Konferenzen und Einladungen nach Russland ein wohlgesinntes Netzwerk aus europäischen Politikerinnen und Politikern aus dem ganzen politischen Spektrum. China indes instrumentalisiert die chinesische Diasporagemeinschaft verdeckt, um seine Interessen zu verteidigen und zu fördern. Es verschafft sich zudem Einfluss, indem es nicht-chinesische Schlüsselakteure mit oder ohne deren Wissen für seine Zwecke einspannt. Medien, Politikerinnen und Politiker, Verwaltungen, Privatwirtschaft und Unternehmerinnen und Unternehmer, Universitäten und Verbände können Ziele solcher Bemühungen sein.

Die zunehmende Digitalisierung und die damit einhergehende breite Palette an technologischen Mitteln ermöglichen es, Informationen günstig und transnational einer breiten Masse zugänglich zu machen. Nutzerinnen und Nutzer können dabei nicht nur Empfänger von Informationen sein, sondern können digitale Inhalte teilen, kommentieren und «liken» und Desinformation so zu grösserer Reichweite verhelfen – unbewusst oder bewusst, etwa um Klicks und Aufmerksamkeit zu generieren. Insbesondere in sozialen Medien ist es schwierig, Desinformation und ihre Autorenschaft überhaupt oder gar rechtzeitig zu erkennen. Die EU hat analysiert, dass für Beeinflussung mehrheitlich Bilder und Videos genutzt werden.[5] Russland beispielsweise nutzt digitale Informations- und Kommunikationsmittel rege, um Desinformation zu streuen. Dazu gehören neben sozialen Medien die russischen staatlichen Auslandssender Russia Today (RT) und Sputnik, die in über 30 Sprachen weltweit berichten, auch auf Deutsch und Französisch.

Den Einsatz von manipulativen Methoden und Technologien können auch private Akteure der «*influence-for-hire*»-Industrie begünstigen, welche verschiedene Dienstleistungen und Softwareprodukte

[4] Meta, Meta's Adversarial Threat Report, Fourth Quarter 2022, 23. Februar 2023, <https://about.fb.com/news/2023/02/metas-adversarial-threat-report-q4-2022> (aufgerufen am 21. Februar 2024).
[5] EEAS, Report on FIMI Threats, Februar 2023, S. 5, <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf> (aufgerufen am 21. Februar 2024).

zur Unterstützung von Beeinflussungsaktivitäten online vermarkten. Beispielsweise bot das 2022 enttarnte israelische Unternehmen «Team Jorge» die Manipulation von Wahlen an, auch mittels Desinformation.

Nicht-authentische Konten sogenannter Internet-Trolle und Bots können in sozialen Medien und Online-Foren Debatten lancieren, Aussagen in Frage stellen oder Gerüchte streuen. Im Auftrag von Staaten agierende reale Personen, die sich unter falscher Identität als normale Nutzerinnen und Nutzer ausgeben, oder sogenannte «*Social Bots*» können viele Beiträge generieren und so den falschen Eindruck erwecken, dass viele Menschen eine bestimmte Meinung vertreten. Computerprogramme können beispielsweise standardisierte Antworten auf gewisse Themen automatisch in Foren publizieren.

Das Unternehmen Meta identifizierte Ende August 2023 ein Netzwerk von 7704 gefälschten Konten, 954 Seiten und Gruppen auf Facebook sowie 15 Konten auf Instagram, welche Desinformation im Auftrag Chinas verbreitet hätten. Das Netzwerk zielte vor allem darauf ab, positive Kommentare über China und die Provinz Xinjiang, wo der chinesische Staat umfassende Repression gegen die uigurische Minderheit betreibt, sowie Botschaften zu verbreiten, die auf die USA, westliche Regierungen und regierungskritische Journalisten und Wissenschaftler in China abzielten.[6]

Digitalen Plattformen kommt demnach eine tragende Rolle bei der Verbreitung von Desinformation zu. Oftmals intransparente Algorithmen auf Plattformen und Suchmaschinen können Inhalte basierend auf den Vorlieben und Interessen der Nutzerinnen und Nutzer empfehlen und vielgeteilte Inhalte prominenter platzieren. Wenn jemand bereits mit Desinformation interagiert hat oder ein dafür empfängliches Nutzerprofil aufweist, werden oft ähnliche Inhalte vorgeschlagen. Hier zeigt sich, dass die Offenheit des Internets und die niedrigen technischen Zugangsbarrieren bei gleichzeitiger Abwesenheit einer journalistisch-redaktionellen Auswahl von Informationen zur verstärkten Verbreitung von Desinformation führen können.[7] Desinformation wird auf digitalen Plattformen und Medienportalen auch verbreitet, weil es beteiligten Unternehmen Klicks und damit Einnahmen generiert. So verbreiten reale oder erfundene Medienorganisationen ungenügend geprüfte Inhalte, beispielsweise mit reisserischen Überschriften oder irreführenden Vorschaubilder («*Clickbait*»).

Die Geschäftsbedingungen und die Moderationsleistungen unterscheiden sich zwischen Plattformen erheblich. Als Reaktion auf gewisse Einschränkungen, etwa das Verbot von RT und Sputnik durch die EU oder das Sperren vieler ihrer falschen Konten auf sozialen Medien, setzt Russland im Internet vermehrt auf alternative Kanäle, etwa über leicht angepasste Internetadressen oder neu geschaffene Plattformen. Seit Beginn des Kriegs in der Ukraine ist ein Zuwachs russischer Propagandainhalte in europäischen Sprachen auf kaum regulierten, nicht-westlichen Plattformen wie TikTok und Telegram festzustellen.

Die rasante Entwicklung und Verbreitung von KI drohen das Potenzial von Beeinflussungsaktivitäten quantitativ und qualitativ dramatisch zu vergrössern. KI automatisiert viele der Prozesse, die zur Entwicklung und Verbreitung von Desinformation notwendig sind. Ein Beispiel sind Deep Fakes. Deep Fakes bezeichnen Videos, Bilder oder Audiodateien, die mithilfe von KI und oftmals unter geringem Mittel- und Zeitaufwand manipuliert wurden, um Personen oder Ereignisse täuschend echt zu fälschen. Diese können wiederum auf allen gängigen Kanälen, vor allem unmoderierten sozialen Medien, eingesetzt werden. Mittel wie *Large Language Models* (LLMs) vereinfachen die Nutzung von Benutzerkonten unter falscher Identität und die Imitation sozialer Bewegungen («*Astroturfing*»). Diese nutzen immer bessere Sprachmodelle und sind von Menschen und Regulierungs- und Aufsichtsbehörden immer schwieriger als künstlich generiert zu erkennen.

---

[6] The Guardian, Meta closes nearly 9,000 Facebook and Instagram accounts linked to Chinese ‘Spamouflage’ foreign influence campaign, 29. August 2023; <https://www.theguardian.com/australia-news/2023/aug/30/meta-facebook-instagram-shuts-down-spamouflage-network-china-foreign-influence> (aufgerufen am 23. Februar 2024).
[7] Vgl. *Saurwein/Spencer-Smith,* Inhaltsregulierung auf Internet-Plattformen. Optionen für verantwortungsorientierte Governance auf nationaler Ebene, S. 42.

2.4 Mögliche Effekte

Alle Beeinflussungsaktivitäten beruhen auf der Grundannahme, dass Aktivitäten im Informationsraum einen Einfluss auf das Denken, die Diskurse und das Handeln von Menschen haben können. Beeinflussungsaktivitäten im Informationsraum können das Vertrauen in Institutionen, die unbeeinflusste Meinungsbildung und freie Entscheidfassung, und damit die Handlungsfähigkeit von Staaten, demokratische Prozesse und die nationale Sicherheit beeinträchtigen – selbst wenn sie jeweils nur einen kleinen Teil der Bevölkerung erreichen. Grundsätzlich ist zwischen kurz-, mittel- und langfristigen Effekten zu unterscheiden; kurzfristig beispielsweise die Meinungsbildung zu einer Abstimmung, mittelfristig etwa der Ton, Charakter und Grad an Polarisierung im politischen Diskurs eines Landes, und langfristig etwa das Vertrauen in Institutionen.

Die genaue Wirkung von Beeinflussungsaktivitäten zu messen, ist schwierig, beispielswiese die Effekte von Beeinflussungsaktivitäten durch Staaten mittels sozialer Medien.[8] In der Wissenschaft und in den Medien werden entsprechend ihre möglichen Effekte unterschiedlich eingeschätzt, ebenso, welche Konstellationen an Desinformationsinhalten, Timing, Verbreitbarkeit und Kontextfaktoren diese begünstigen. Besonders relevant sind die Effekte anhaltender, möglicherweise koordinierter Beeinflussungsaktivitäten und Desinformation, nicht von einzelnen Aktivitäten.

Beeinflussungsaktivitäten und Desinformation können dazu beitragen, das Vertrauen in Politikerinnen und Politiker – allgemein Personen des öffentlichen Lebens –, Medien, Institutionen und Informationen an sich nachhaltig zu beschädigen. Beeinflussungsaktivitäten können die freie Willens- und Meinungsbildung in demokratischen Prozessen beeinträchtigen. Betroffene können sich von der Politik abwenden, weil ihr Vertrauen in Informationen und Prozesse erodiert ist. Mangelndes Vertrauen in demokratische Institutionen und Prozesse kann zu einer erschwerten Kommunikation und Kompromissfindung über politische Gräben hinweg führen, da die gemeinsame Basis an Tatsachen als Grundlage für politische Auseinandersetzungen infrage gestellt ist. Beeinflussungsaktivitäten können z. B. das Vertrauen in die Polizei- und Strafverfolgungsbehörden untergraben, indem sie den Eindruck erwecken, die Behörden würden einseitig ermitteln, willkürlich handeln oder seien «unterwandert». Im schlimmsten Fall kann es zur Radikalisierung von Betroffenen führen.

Die strukturelle und nachhaltige Wirkung von Beeinflussungsaktivitäten kann wiederum den Boden bereiten für allfällige kurzfristige Effekte, beispielsweise die Mobilisierung zu politischen Aktionen oder Gewaltanwendung. Zudem beschränken Beeinflussungsaktivitäten und die Verbreitung von Desinformation manchmal die Handlungsfreiheit von Behörden, indem sie Ressourcen binden, gerade in Zeiten von Krisen und Unsicherheit.

Verschiedene Beispiele zeigen Beeinflussungsaktivitäten durch andere Staaten und ihre Effekte auf die Resilienz demokratischer Institutionen. Russische Konten auf Facebook und X/Twitter verbreiteten Desinformation rund um das britische Brexit-Referendum und die US-Präsidentschaftswahlen von 2016.[9] Frankreich wurde 2017 während der Präsidentschaftswahl Ziel von russischen Beeinflussungsaktivitäten in Form von Leaks sensiblen Materials zur Desavouierung des Spitzenkandidaten Emmanuel Macron.

Zu von russischen Akteuren verbreiteten Inhalten gehören z. B. Migration, die Abkehr von traditionellen Familienstrukturen, Kritik an Waffenlieferungen an die Ukraine oder diskriminierende Polizeigewalt. Diese Themen finden sich auch in authentischen Meinungen, Ängsten und Forderungen in der Gesellschaft wieder. Die genaue Abgrenzung dessen, was freier Meinungsbildung und was Manipulation und vorsätzlicher Täuschung entspringt und deshalb überzeichnet ist, ist deshalb schwierig. Beeinflussungsaktivitäten im Informationsraum gehen in gewissen Politikbereichen einher mit anderen Mitteln hybrider Konflitkführung, beispielsweise als das belarussische Regime im Herbst 2021 Migrantinnen und Migranten aus dem Nahen und Mittleren Osten beim Grenzübertritt nach Polen und Litauen gezielt unterstützte. Dies war von Desinformation in russischen Medien über die angeblich völlige Dysfunktionalität europäischer Asyl- und Migrationssysteme begleitet. Es gelingt Russland aber derzeit in westlichen Staaten kaum, die gesellschaftliche Mehrheitsmeinung und die politischen Entscheidungen – etwa zum Krieg in der Ukraine – massgebend zu beeinflussen.

---

[8] Jon Bateman, Elonnai Hickok et al, Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research, 28. Juni 2021, <https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824> (aufgerufen am 5. April 2024).

[9] *Bayer et al.,* Disinformation and propaganda.

Desinformation während der COVID-19-Pandemie appellierte an Skepsis gegenüber staatlichen Stellen und an Emotionen und Ängste. Desinformation kann entsprechend auch dazu führen, dass Menschen Gesundheitshinweise offizieller Stellen ignorieren und gesundheitliche Risiken eingehen. Damit hat sie eine sicherheitspolitische Relevanz und kann sich auch auf die wirtschaftliche und finanzielle Lage eines Landes auswirken. Solche Effekte sind auch kurzfristig denkbar. Ein durch KI generiertes Bild eines angeblich brennenden US-Regierungsgebäudes etwa zirkulierte im Mai 2023 innert Minuten über Facebook und X/Twitter, einschliesslich der Konten der russischen RT. Ein kurzfristiges Tagestief an US-Börsen an diesem Tag wird teilweise darauf zurückgeführt.[10]

Beeinflussungsaktivitäten und Desinformation können sich auch auf die Friedensförderung und humanitäre Bemühungen auswirken. UNO-Friedensförderungsmissionen in Mali, der Zentralafrikanischen Republik und der Demokratischen Republik Kongo sind bzw. waren von Desinformation betroffen. In der Zentralafrikanischen Republik unterstellte Online-Desinformation u. a. mit gefälschtem Videomaterial vier UNO-Mitarbeitenden, Waffen an Rebellen zu liefern, und rief zu Gewalt gegen die Mission auf.[11] Solche Desinformation trägt bei der lokalen Bevölkerung zu Ressentiments bei, welche in Gewalt ausarten können. Dies gefährdet die Sicherheit des Personals internationaler Missionen und die Förderung von Sicherheit und Frieden im Land.[12] Auch humanitäre Organisationen wie das Internationale Rote Kreuz können von solchen Aktivitäten betroffen sein.

3. Beurteilung und Bewältigung im internationalen Vergleich

Eine zunehmende Anzahl Staaten und internationale Organisationen (z. B. die NATO, EU) haben in den letzten Jahren Beeinflussungsaktivitäten im Informationsraum als Herausforderung für ihre Sicherheit erkannt. Diejenigen, die sich besonders betroffen fühlen, sind in ihren Massnahmen etwas weiter vorangeschritten – wie beispielsweise die USA, das Vereinigte Königreich, Frankreich oder Deutschland aufgrund ihrer internationalen Präsenz oder Australien, die nordischen und baltischen Staaten aufgrund ihrer geographischen Nähe zu China bzw. Russland. Aufgrund der transversalen Auswirkungen bestehen auch auf internationaler Ebene Bemühungen für eine verstärkte Zusammenarbeit und Koordination.

Grundsätzlich ist festzuhalten, dass viele Gegenmassnahmen noch begrenzt erprobt sind und ihre Ausgestaltung und Effektivität stark vom nationalen Kontext abhängig sind. Die folgenden Ansätze haben keinen Anspruch auf Vollständigkeit.

3.1 Strategische Beurteilung

Australien, Deutschland, Frankreich, die Niederlande, Kanada, Österreich, das Vereinigte Königreich und die USA beurteilen Beeinflussungsaktivitäten und Desinformation als strategische Bedrohung; die Niederlande dies explizit als Bedrohung der nationalen Sicherheit[13]. Deutschland (Nationale Sicherheitsstrategie vom Juni 2023) und Frankreich (*Actualisation stratégique 2021*) heben die Bedrohung für demokratische Willensbildungsprozesse hervor. Auch die USA und das Vereinigte Königreich betonen das Risiko der ungebührlichen Einflussnahme auf freie politische Meinungsbildung durch Desinformation, wobei sie die Kombination mit neuen Technologien und *big data* als besonders besorgniserregend erachten (*US 2023 Annual Threat Assessment*; *UK Integrated Review of Security, Defence, Development and Foreign Policy 2021*). Handlungsbedarf sehen diese Staaten insbesondere bei der frühzeitigen Erkennung sowie der Stärkung der Resilienz von Institutionen und der Gesellschaft. Deutschland beabsichtigt, zwei Strategien auszuarbeiten: eine zur Steigerung der Handlungsfähigkeit gegenüber hybriden Bedrohungen und eine zum Umgang mit Desinformation. Österreich setzt auf den Auf- und Ausbau zivil-

---

[10] The New York Times, An A.I.-Generated Spoof Rattles the Markets, 23. Mai 2023, <https://www.nytimes.com/2023/05/23/business/ai-picture-stock-market.html#:~:text=Fake%20news%2C%20real%20market%20drop,investor%20fears%2C%20sending%20stocks%20tumbling> (aufgerufen am 21. Februar 2024).
[11] Albert Trithart, Disinformation against UN Peacekeeping Operations, International Peace Institute, November 2022, S. 3, <https://www.ipinst.org/wp-content/uploads/2022/11/2212_Disinformation-against-UN-Peacekeeping-Ops.pdf> (aufgerufen am 21. Februar 2024).
[12] So gaben in einer Umfrage 75 % der befragten UN-Friedensförderer an, dass Desinformation Auswirkungen auf ihre Sicherheit habe. Siehe Ibid., S. 13.
[13] The Security Strategy for the Kingdom of the Netherlands, 3. April 2023, <https://www.government.nl/binaries/government/documenten/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands/Security+Strategy+for+the+Kingdom+of+the+Netherlands.pdf> (aufgerufen am 21. Februar 2024).

militärischer Kooperationsformate sowie die Intensivierung der Zusammenarbeit mit anderen EU-Mitgliedstaaten.

Die EU entwickelte auf Grundlage ihres Strategischen Kompasses für Sicherheit und Verteidigung von 2022 ein Instrumentarium zur Bekämpfung ausländischer Einflussnahme und Informationsmanipulation (FIMI; *Foreign Interference and Information Manipulation Toolbox*). Dieses umfasst die Verbesserung der Lagebeurteilung und Frühwarnung, die Stärkung der gesellschaftlichen Resilienz sowie regulatorische und restriktive Massnahmen im Rahmen geografischer Sanktionsregime. Ab 2024 sollen alle unter der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU laufenden Missionen und Operationen fähig sein, Informationsmanipulation und ausländischer Einflussnahme zu begegnen. Die Nato wird gemäss ihrem Strategischen Konzept 2022 in ihre Fähigkeit investieren, sich auf hybride Bedrohungen wie Desinformation und Einflussnahme vorzubereiten. Aufgeschreckt durch die zunehmenden Risiken für internationale Missionen zur Friedensförderung ist auch das Bewusstsein der UNO in den letzten Jahren gestiegen. Im Juli 2022 drückte der UNO-Sicherheitsrat seine Besorgnis über die zunehmenden Auswirkungen von Desinformation auf Friedensförderungsmissionen aus. Die Sonderberichterstatterin für die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäusserung widmete ihre letzten beiden Berichte Aspekten von Desinformation.[14]

3.2 Lagebeobachtung und Früherkennung

Verschiedene Staaten haben Institutionen spezifisch zur Früherkennung geschaffen. Im Juli 2021 hat Frankreich die Organisation Viginum (*Vigilance et Protection Contre les Ingérences Numériques étrangères*) gegründet. Auf Basis öffentlich zugänglicher Quellen analysiert Viginum Muster ausländischer Einflussnahme insbesondere im Vorfeld von Wahlen. Schweden hat 2022 eine sogenannte psychologische Verteidigungsagentur[15] geschaffen mit dem Ziel, ausländische Einflussnahme im Informationsraum zu identifizieren, zu analysieren und zu bekämpfen sowie die Resilienz der Bevölkerung zu stärken. Auch im Vereinigten Königreich analysiert und erforscht ein Direktorat im Aussenministerium öffentlich zugängliche Informationen und formuliert entsprechende Strategien und Gegenmassnahmen. Eine *Defending Democracy Taskforce* fokussiert spezifisch auf die frühzeitige Identifizierung der Gefährdung von Wahlen durch Beeinflussungsaktivitäten im Informationsraum. In den USA beobachtet das *Global Engagement Center* die Lage und stellt durch Russland verbreiteten Narrativen Fakten gegenüber.[16]

Die sieben führenden Industrienationen (G7) haben 2018 unter Führung Kanadas den *G7 Rapid Response Mechanism* eingerichtet, um den Informationsraum zu analysieren und Bedrohungen zu identifizieren. Der Mechanismus sieht auch gemeinsame Massnahmen und Koordination vor. In diesem Gremium sind Australien, Neuseeland, die Niederlande, die Nato und Schweden als Beobachter vertreten. Das *Rapid Alert System* im Europäischen Auswärtigen Dienst der EU (EEAS) fördert den Informationsaustausch zwischen den Mitgliedstaaten. Mit EUvsDisinfo[17] analysiert und veröffentlicht eine Informationsplattform der EU gängige Narrative, um die Bevölkerung zu sensibilisieren. In seinem zweiten Bericht zu FIMI vom Januar 2024 wies der EEAS für die Zeit zwischen Dezember 2022 und November 2023 750 einzelne Vorfälle von Beeinflussungsaktivitäten aus.[18]

3.3 Resilienz durch Sensibilisierung, Bildung und Medienkompetenz

Die Stärkung der eigenen Resilienz und ein gesamtgesellschaftlicher Ansatz sehen demokratische Regierungen wie Forschung als wichtigste, aber auch herausfordernde Massnahme zur Bekämpfung von Beeinflussungsaktivitäten im Informationsraum. Bei einer Vielzahl von Initiativen stehen insbesondere die Sensibilisierung der Gesellschaft, die Stärkung der Medienkompetenz in der Bevölkerung und der Medienqualität im Vordergrund.

---

[14] OHCHR, Disinformation and freedom of opinion and expression during armed conflicts, 12. August 2022, <https://www.ohchr.org/en/documents/thematic-reports/a77288-disinformation-and-freedom-opinion-and-expression-during-armed>; OHCHR, Freedom of expression and the gender dimensions of disinformation, 7. August 2023, <https://www.ohchr.org/en/calls-for-input/2023/report-freedom-expression-and-gender-dimensions-disinformation>.
[15] Myndigheten för psykologiskt försvar (Psychological Defence Agency)
[16] <https://www.state.gov/disarming-disinformation/#reports>
[17] <https://euvsdisinfo.eu/de/>
[18] Europäischer Auswärtiger Dienst, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, Januar 2024, <https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en> (aufgerufen am 5. März 2024)

Deutschland baut ein Zentrum für Strategie, Analyse und Resilienz auf, in welchem das Innen-, Aussen- und Verteidigungsministeriums vertreten sind. Schweden arbeitet mit zivilgesellschaftlichen Organisationen, Forschungsinstitutionen, Medien und Gemeinden zusammen, um Beeinflussungsaktivitäten im Informationsraum zu begegnen und die Bevölkerung zu sensibilisieren, und investiert jährlich 1,2 Millionen Euro[19] in die Forschung. Das Vereinigte Königreich hat sich in den letzten Jahren mittels regulatorischer Initiativen und Kampagnen bemüht, die Medienkompetenz der Bevölkerung zu stärken. In Australien sind ähnliche Arbeiten zu beobachten.

Das *European Digital Media Observatory* (EDMO) ist ein von der EU finanziertes Netzwerk, das Akteure wie Medien, Plattformen, Zivilgesellschaft und Forschung zusammenbringt, Desinformationskampagnen analysiert, Massnahmen der Tech-Industrie überwacht und die Medienkompetenz der Bevölkerung stärkt. EDMO ist bei der Überarbeitung und Evaluation des *Strengthened CoP* der EU involviert (siehe 3.4).

Weitere gemeinsame Initiativen von Staaten, bei denen auch die Schweiz mitwirkt, zielen auf die Stärkung des Schutzes der Privatsphäre und des Zugangs zu verlässlichen Informationen sowie den Schutz von Journalisten und Medienschaffenden, beispielsweise die *Media Freedom Coalition*, die Koalition für Internetfreiheit und den Schutz der Menschenrechte (*Freedom Online Coalition*) oder die Partnerschaft für Information und Demokratie.

3.4 Regulierung und Sanktionen

Zahlreiche Staaten haben Initiativen zur Regulierung digitaler Plattformen ergriffen. Die Ansätze umfassen ein breites Spektrum von staatlicher Regulierung über Co-Regulierung bis hin zu Selbstregulierung. Die gesetzgeberischen Ansätze konzentrieren sich auf die Entfernung von für schädlich befundenen Inhalte oder deren Kennzeichnung, die Transparenz von Werbung, die Stärkung der Rechte von Nutzerinnen und Nutzern, und die Unterstützung von Forschung. Die USA haben auf Basis des *2020 National Defence Authorization Act* eine Behörde gegründet, das *Social Media Data and Threat Analysis Center*, welche die Koordination mit den Plattformen sozialer Medien sicherstellt.

Auf EU-Ebene trat im August 2023 mit dem Gesetz über Digitale Dienste (*Digital Services Act*, DSA) eine neue Regulierung in Kraft, welche die Plattformen teilweise eigenständig umsetzen. Der DSA soll die Verbreitung illegaler Inhalte im digitalen Raum verhindern und die Grundrechte der Nutzenden schützen. Desinformation ist teilweise abgedeckt, wo es um Hassrede und andere illegale Äusserungsdelikte oder um die Bedrohung der öffentlichen Sicherheit geht. Im Kontext des Kriegs zwischen Israel und der Hamas forderte die Europäische Kommission im Oktober 2023 von Meta und TikTok formell Auskunft zu ihren Massnahmen gegen die Verbreitung von Desinformation. Ferner beschleunigte sie die Überwachung und Durchsetzung des DSA, einschliesslich eines Koordinationsmechanismus zwischen den Mitgliedstaaten gegen die Verbreitung illegaler Inhalte.

Mit einem freiwilligen Verhaltenskodex für Technologie- und Werbeunternehmen will die Europäische Kommission gegen Desinformation in den sozialen Medien vorgehen. Diesen *EU Code of Practice (CoP) on Disinformation* haben bis jetzt 40 Unternehmen unterzeichnet; er wurde aufgrund mangelnder Effektivität überarbeitet zum *Strengthened Code of Practice* und schliesst eine permanente Task Force[20] ein. Auch die UNO setzt auf einen Verhaltenskodex, um der digitalen Verbreitung von Desinformation entgegenzuwirken. Dieser soll staatliche und nichtstaatliche Akteure dazu aufrufen, gegen Desinformation vorzugehen und die Menschenrechte zu respektieren. Einige Länder wählen auch direkte regulatorische Ansätze. So hat die norwegische Regierung einen Gesetzesentwurf vorgeschlagen, der die Beteiligung an Beeinflussungsaktivitäten im Auftrag ausländischer Nachrichtendienste unter Strafe stellen soll. Verschiedene Länder – etwa Brasilien, Frankreich, Kambodscha, Kenia und Kroatien – haben Gesetze gegen Online-Desinformation im Zusammenhang mit Wahlen erlassen. Viele solcher Gesetzeserlasse waren von Sorgen und Protesten um Meinungs- und Medienfreiheit begleitet und wurden in einigen weiteren Staaten wieder zurückgezogen.

---

[19] Jean-Bapiste Jeangène Vilmer: Effective State Practices against disinformation: Four country case studies. Hybrid CoE Research Report 2 (July 2021), S. 12.

[20] Mitglieder der Task Force sind die Unterzeichnenden, die Europäische Regulierungsgruppe für audiovisuelle Mediendienste, Europäische Beobachtungsstelle für digitale Medien und der Europäische Auswärtige Dienst. Vorsitzende ist die EU-Kommission.

Das von der EU entwickelte Instrumentarium (*FIMI Toolbox;* siehe 3.1) umfasst im Rahmen von geographischen Sanktionsregimen restriktive Massnahmen gegen Unternehmen und Personen, die für Beeinflussungsaktivitäten im Informationsraum verantwortlich sind. So haben die EU und ihre Mitgliedstaaten im Kontext des Kriegs gegen die Ukraine Sanktionen gegen russische Personen und Entitäten verhängt (Einreisesperren, Einfrieren von Vermögenswerten, Verbot der Bereitstellung von Geldern oder wirtschaftlichen Ressourcen, Lizenzentzug). Darunter fallen fünf Sender von RT sowie Sputnik. Am 28. Juli 2023 sanktionierte die EU weitere sieben Personen und fünf Entitäten wegen Informationsmanipulation.[21] Am 30. Mai 2023 und am 22. Februar 2024 verhängte die EU Sanktionen gegen Unternehmen und Personen aus Moldau für die Destabilisierung der Republik, u.a. durch Desinformation.[22]

Mehrere Staaten, darunter das Vereinigte Königreich, die USA und Australien, haben Beeinflussungsagenten und -agentinnen sowie deren Plattformen mit Sanktionen belegt. Führende westliche Social-Media-Unternehmen wie Facebook, YouTube und X/Twitter schränkten in unterschiedlichem Ausmass den Zugang zu und die Verbreitung von Inhalten aus staatsnahen russischen Quellen ein.

3.5 Zuständigkeiten, Koordination und Kommunikation

Da Beeinflussungsaktivitäten im Informationsraum zahlreiche Themenbereiche und Kompetenzen betreffen, sind die Zuständigkeiten in Regierungen sehr unterschiedlich geregelt und auf viele Ministerien verteilt, was Koordination bedarf.

In Frankreich liegt die Federführung beim Büro des Premierministers, wo auch Viginum angegliedert ist. Ein wissenschaftliches Ethikkomitee überwacht die Tätigkeit der Organisation. In Deutschland ist das Innenministerium verantwortlich für die Themen Desinformation und Einflussnahme. Dieses koordiniert eine interdepartementale Arbeitsgruppe. In Schweden ist die Behörde zur psychologischen Verteidigung im Verteidigungsministerium angesiedelt. Auch die baltischen Staaten wollen Beeinflussungsaktivitäten und Desinformation explizit gesamtstaatlich begegnen, einschliesslich die Förderung von Medienkompetenz der Bevölkerung und die Integration von Minderheiten, namentlich der russischen. Im Vereinigten Königreich koordiniert das Aussenministerium die Tätigkeiten, wobei verschiedene Stellen in der Regierung sich ebenfalls mit dem Thema aus ihrer Perspektive befassen; ähnlich in den USA, wo das *Global Engagement Center* dem Aussenministerium angegliedert ist und den Auftrag hat, die Bemühungen der Regierung zur Bekämpfung von Desinformation zu koordinieren. In der EU beraten über 40 Mitarbeitende des EEAS die Union und ihre Mitgliedstaaten im Umgang mit illegitimer Einflussnahme und Desinformation durch ausländische Akteure und erarbeiten jährliche Berichte.

Migration ist ein wiederkehrendes Thema von Desinformation, und Migrationsbewegungen können zur hybriden Konfliktführung instrumentalisiert werden. Angesichts dessen schlug die Europäische Kommission 2021 eine Regelung zu Situationen vor, in der ein Drittland irreguläre Migrationsbewegungen in die EU auslöst, um diese oder einen Mitgliedstaat zu destabilisieren.[23]

Verschiedene Staaten haben die strategische Kommunikation verstärkt, um Beeinflussungsaktivitäten im Informationsraum zu begegnen, etwa im Rahmen der Nato. Strategische Kommunikation umfasst ein Bündel koordinierter kommunikativer Aktivitäten, welches die eigenen Ziele, Interessen und das Vorgehen vermitteln und legitimieren soll und damit gegnerischen Narrativen begegnet. Die EU hat im EEAS eine Stelle spezifisch für strategische Kommunikation definiert. Die Nato wird in ihren Bemühungen

---

[21] Rat der EU, Pressemitteilung, Information manipulation in Russia's war of aggression against Ukraine: EU lists seven individuals and five entities, 28. Juli 2023, <https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/> (aufgerufen am 21. Februar 2024).

[22] Rat der EU, Pressemitteilung, Republic of Moldova: 7 individuals listed for their destabilising actions and for undermining the territorial integrity of Ukraine, 30. Mai 2023, <https://www.consilium.europa.eu/en/press/press-releases/2023/05/30/republic-of-moldova-7-individuals-listed-for-their-destabilising-actions-and-for-undermining-the-territorial-integrity-of-ukraine/>; Rat der EU, Pressemitteilung, Republic of Moldova: six individuals and one entity listed for undermining the rule of law, stability and security in the country, 22. Februar 2024, <https://www.consilium.europa.eu/en/press/press-releases/2024/02/22/republic-of-moldova-six-individuals-and-one-entity-listed-for-undermining-the-rule-of-law-stability-and-security-in-the-country/> (aufgerufen am 18. März 2024).

[23] Dies massgeblich vor dem Hintergrund, dass Belarus im Herbst 2021 irreguläre Migration nach Polen und Litauen förderte; Europäische Kommission, Generaldirektion Migration und Inneres, Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Bewältigung von Situationen der Instrumentalisierung im Bereich Migration und Asyl, 2021/0427/COD, <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52021PC0890> (aufgerufen am 5. März 2024).

durch ein unabhängiges Kompetenzzentrum, das *NATO Strategic Communications Center of Excellence*, unterstützt.

4. Betroffenheit der Schweiz

4.1 Bedrohungslage

Mit ihrem direktdemokratischen System, wo die Bevölkerung regelmässig politische Entscheide fällt, mit einigen potenziellen gesellschaftlichen und politischen Bruchlinien sowie als aussenpolitische Akteurin und Gastgeberin zahlreicher internationaler Organisationen kann die Schweiz für Beeinflussungsakteure ein geeignetes Ziel sein. Die Schweiz ist als Staat in Europa und Teil der westlichen Wertegemeinschaft sowie wegen ihrer starken internationalen wirtschaftlichen und politischen Vernetzung schon länger indirekt Ziel von allgemeinen, auf westliche Staaten abzielenden Beeinflussungsaktivitäten. Sie ist aber zunehmend auch direktes Ziel von auf sie zugeschnittenen Aktivitäten. Es gibt indes keine Hinweise, wonach eidgenössische Urnengänge ein direktes Ziel von Beeinflussungsaktivitäten gewesen wären.

Für die Schweiz stehen im Zusammenhang mit Beeinflussungsaktivitäten Russland, aber auch China, als mutmassliche Urheber im Vordergrund.[24] Seit Russland die Schweiz nach der Verhängung von Sanktionen im Zusammenhang mit dem Krieg gegen die Ukraine auf seine Liste «unfreundlicher Staaten» gesetzt hat, nahmen auf sie zugeschnittene russische Desinformationsaktivitäten zu, zuletzt etwa im Kontext der Hochrangigen Konferenz zum Frieden in der Ukraine durch die Schweiz im Sommer 2024. Auch wenn die russischen Auslandsmedien keine Schweiz-spezifischen Plattformen bewirtschaften, können deren mehrsprachige Inhalte die Schweizer Bevölkerung erreichen; der Bundesrat beurteilt deren Reichweite aber letztlich als gering. Russische Beeinflussungsaktivitäten dürften sich intensivieren, wenn politische Debatten oder der Ausgang von politischen Prozessen in der Schweiz wie Volksabstimmungen von besonderer Bedeutung für Russlands Interessen sind. Dazu können Debatten über die Energieversorgung, die Neutralität, Sanktionen, die Unterstützung der Ukraine oder die mögliche Verwendung eingefrorener russischer Zentralbankvermögen gehören.

Die Thematik wird in der Schweiz in Politik, Medien und Gesellschaft zunehmend wahrgenommen und diskutiert. Die Schweizer Bevölkerung ist und fühlt sich mit Desinformation konfrontiert. Die Internetnutzungsumfrage 2021 des Bundesamts für Statistik (BFS) zeigt, dass fast die Hälfte der Bevölkerung (45 %) angibt, auf Nachrichtenseiten oder in sozialen Netzwerken fragwürdige Informationen gesehen zu haben. Folglich ist die Hälfte der Mediennutzenden der Meinung, keine fragwürdigen Inhalte gesehen zu haben, bzw. hat diese nicht als solche erkannt. Gemäss dem Bericht «Desinformation in der Schweiz 2021»[25] im Auftrag des Bundesamtes für Kommunikation (BAKOM) hält fast die Hälfte der Befragten Desinformation für ein grosses oder sehr grosses Problem. Laut dem Bericht stellt Desinformation ein grosses Problem für das Vertrauen in die Medien, die Politik und die Behörden sowie für den sozialen Zusammenhalt dar. Inwieweit Beeinflussungsaktivitäten tatsächlich bereits zu solchen Effekten geführt haben, ist schwierig festzustellen. Die negativen Folgen für gesellschaftliche Polarisierung, für die regelbasierte internationale Ordnung und internationale Friedensförderung (siehe 2.3) tangieren auch die politischen und wirtschaftlichen Interessen der Schweiz.

Hervorzuheben ist das Bedrohungspotenzial von Beeinflussungsaktivitäten für die Schweiz als aussenpolitische Akteurin und als Standort zahlreicher internationaler Organisationen. Mit ihrem Vereins- und Stiftungsaufsichtsrecht, in dem die Selbstkontrolle eine wichtige Rolle spielt, könnte das Risiko der Finanzierung von Beeinflussungsaktivitäten über die Schweiz zunehmen. So finanzierte der zum engen Freundeskreis von Putin gehörende Wladimir Jakunin seine Einfluss- und Lobbyorganisation «Dialog der Zivilisationen» über ein Netzwerk von Stiftungen in der Schweiz. Auch die Gründung von als wissenschaftlich bezeichneten Instituten oder medienkritischen Internetportalen ist zu beobachten, die aufgrund des Standorts Schweiz den Anschein besonderer Glaubwürdigkeit zu erheischen hoffen.

---

[24] Sicherheitspolitischer Bericht 2021 des Bundesrats, BBl 2021 2895, und Zusatzbericht vom September 2022, BBl 2022 2357.
[25] Vogler, D., Schwaiger, L., Schneider, J., Udris, L., Siegen, D., Marschlich, S., Rauchfleisch, A., Eisenegger, M. (2021), Falschinformationen, Alternativmedien und Verschwörungstheorien – Wie die Schweizer Bevölkerung mit Desinformation umgeht, Bericht für das Bundesamt für Kommunikation.

4.2 Fallbeispiele

Zwei bekannte Beispiele illustrieren die Inhalte, Narrative und Abläufe solcher Beeinflussungsaktivitäten und die Betroffenheit der Schweiz: Desinformation rund um das Labor Spiez 2018 und ein falsches Energieplakat 2022. Sie zeigen, wie die Schweiz im Rahmen von grösseren, europaweiten Kampagnen direktes Ziel wurde.

Im März 2018, nachdem russische Agenten den ehemaligen russischen Spion Sergei Skripal und seine Tochter im Vereinigten Königreich mit Nowitschok vergifteten, rückte das Labor Spiez in den Fokus der Weltöffentlichkeit, weil es – wie auch andere Labors – im Rahmen der Organisation für das Verbot chemischer Waffen (OPCW) Proben zum Vorfall analysierte. Staatliche, staatlich beauftragte und nichtstaatliche russische Akteure versuchten in sozialen und staatlich kontrollierten Medien die Glaubwürdigkeit des Labors und seiner Analyseergebnisse zu untergraben und die Verantwortung für den Giftanschlag anderen Akteure zuzuschreiben. Der russische Aussenminister Sergei Lawrow behauptete, das Labor Spiez habe Nowitschok-Proben nicht als solche identifiziert. Viele westliche Medien berichteten über Lawrows Aussage. Der Bundesrat und das Labor Spiez widersprachen ihm klar. Russische Trollfabriken wie die *Internet Research Agency* waren beteiligt, die Aussage und Desinformation über soziale Medienplattformen wie X/Twitter und Facebook zu verbreiten. Zwei russische Staatsangehörige wurden in den Niederlanden wegen versuchter Spionage gegen das Labor Spiez verhaftet. Die russischen Aktionen gegen das Labor Spiez und die OPCW sollten primär von Russlands Rolle ablenken, aber die Rufschädigung des Labors Spiez und damit der Schweiz wurde in Kauf genommen.

Ein gefälschtes Werbeplakat des Bundes, das über die sozialen Netzwerke X/Twitter und Telegram verbreitet wurde, wies im Herbst 2022 auf eine Belohnung von 200 Franken hin, wenn man Nachbarn denunzierte, die zu viel heizen. Zum Erscheinungszeitpunkt der Fotomontage debattierte die Schweiz intensiv über die drohende Energiemangellage im Zusammenhang mit dem Krieg in der Ukraine. Am 6. September 2022, vier Tage vor der Erstveröffentlichung der Desinformation, publizierte eine Schweizer Tageszeitung einen Artikel über vorgeschlagene neue Verordnungen, wonach Einwohnerinnen und Einwohnern, die ihre Wohnungen auf über 19 Grad heizten, Geld- oder Freiheitsstrafen drohten. Noch gleichentags replizierten internationale Medien, darunter die deutschsprachige RT, diese Meldung. In den Stunden nach ihrer Veröffentlichung im Internet verbreitete sich die Fotomontage rapide über verschiedene soziale Medien und Online-Plattformen, einschliesslich mittels nicht-authentischer Konten, die dem russischen Beeinflussungsnetzwerk zugerechnet werden.

Das darin transportierte Narrativ unterstellte, dass das demokratische System und die Rechtsstaatlichkeit in der Schweiz dysfunktional seien und hierzulande autokratische Zustände herrschten. Die Bevölkerung sollte verunsichert und gespalten werden. Zudem band der Fall bei verschiedenen Behörden Ressourcen. Beim Generalsekretariat des UVEK, dessen Telefonnummer auf der Fotomontage erschien, riefen über 80 Personen an, die dem angeblichen Denunzierungsaufruf nachkommen wollten. Die punktuelle Störung der Arbeit der Bundesverwaltung hatte jedoch keine einschneidenden Auswirkungen und die Aktion erreichte keine kritische Masse in der Gesellschaft.

4.3 Spezifische Charakteristiken und Resilienz der Schweiz

Die Schweiz hat einige Merkmale, die ihre Betroffenheit von Beeinflussungsaktivitäten und Desinformation tendenziell verringern. Das Bild ist jedoch nuanciert.

Die geringe Grösse des Landes und Medienraums, der hohe Lebensstandard, das gute Bildungsniveau, das überdurchschnittlich hohe Vertrauen in die staatlichen Institutionen und die politische Kompetenz, die u.a. auf häufige Volksabstimmungen zurückgeht, tragen zur Stärkung der Widerstandsfähigkeit des Landes und seiner Institutionen bei. Laut dem Bericht «Desinformation in der Schweiz 2021», in dem verschiedene Vergleichsstudien zitiert werden, ist die Schweiz als Land strukturell gesehen resilienter als viele andere. Die wenig polarisierte Gesellschaft und die Medienlandschaft mit vielen qualitativ hochwertigen Medien sind die eine wichtige Erklärung dafür bzw. Ausdruck davon. Das Zusammenspiel von öffentlichen und privaten Medien sowie das Mehrparteiensystem mit seiner auf Konsens basierenden Politik stärken im internationalen Vergleich die Widerstandsfähigkeit der Schweiz gegen Polarisierung

und Populismus im Internet.[26] Eine weitere Studie hält die Schweiz im europäischen Vergleich zudem für weniger von Fake News betroffen wegen ihrer geringen geopolitischen Bedeutung und ihrer sprachlichen Diversität.[27]

Die direkte Demokratie und die föderale Organisation der Schweiz stellen allerdings nicht nur Stärken, sondern auch eine mögliche Verletzlichkeit in Bezug auf Desinformation dar. Die Vielzahl an Abstimmungen auf allen Staatsebenen bietet Beeinflussungsakteuren die Möglichkeit, von Fall zu Fall Einfluss zu nehmen. Die wahl- und abstimmungsorganisierenden Behörden der verschiedenen Staatsebenen haben durch die zahlreichen Urnengänge jedoch grosse Erfahrung aufgebaut, arbeiten eng zusammen und tauschen sich in verschiedenen institutionalisierten Formaten[28], in spezifischen Gremien[29] und auf internationaler Ebene regelmässig aus.[30] Die vom Meinungsforschungsinstitut gfs.bern durchgeführten VOX-Studien zeigen das Vertrauen der Bevölkerung in die Informationen des Bundesrates, insbesondere im Rahmen von Abstimmungen, etwa in die erläuternde Broschüre des Bundesrates (83 %), Zeitungsartikel (81 %) und Fernsehsendungen (72 %).

Die 2022 in Kraft gesetzten Transparenzbestimmungen statuieren sowohl ein Verbot für politische Akteure, anonyme Spenden als auch Spenden aus dem Ausland anzunehmen (vgl. Art. 76*h* BPR). Die Verbote dürften auch einen gewissen Schutz gegen ausländische Beeinflussungsaktivitäten im Informationsraum bieten.

Betrachtet man neben diesen strukturellen Faktoren die Thematik der Beeinflussungsaktivitäten auf der individuellen Ebene, deuten verschiedene Indizien darauf hin, dass die Resilienz der Schweizer Bevölkerung in Bezug auf Desinformation künftig abnehmen könnte. Zwar verfügt die Bevölkerung über ein vergleichsweise hohes Mass an Kompetenzen in Staatskunde. Eine Studie ermittelt bei den Schweizer Befragten jedoch eher tiefe Werte an Medienkompetenz, etwa leicht tiefer als in einer deutschen Vergleichsstudie. Beispielsweise fiel vielen Befragten schwer, die Kommunikationsabsicht (als Information, Kommentar oder Werbung) eines Medienbeitrags zu ermitteln, was bei der Einschätzung von Desinformation zentral sein dürfte. 73 % der Befragten gaben an, von der Masse an verfügbaren Informationen ganz oder teilweise überfordert zu sein.[31] Die Medienkompetenz und damit tendenziell die Resilienz gegenüber Beeinflussungsaktivitäten bei Individuen ist höher bei grösserem Grad an Interesse an Nachrichten, politischer Beteiligung, Nutzung digitaler *und* traditioneller Medien, und Vertrauen in Schweizer Medien allgemein. Ältere Menschen stellen eine für Desinformation besonders vulnerable Gruppe dar, da ihre Medienkompetenz unabhängig vom Bildungsstand gegenüber anderen Altersgruppen tiefer ist.[32]

Gemäss jüngsten Erkenntnissen schreibt sich die Schweizer Bevölkerung im internationalen Vergleich dennoch insgesamt durch eine leicht überdurchschnittliche digitale Medienkompetenz zu. Gemäss der Omnibus-Umfrage 2021 zur Internetnutzung[33] liegt die *Selbsteinschätzung* zur digitalen Kompetenz der

---

[26] Gemäss Tobias Keller, Kommunikations- und Medienwissenschaftler beim Forschungsinstitut gfs.bern, der bei der Studie Digitalisierung der Schweizer Demokratie mitgearbeitet hat. Urs Bieri et. al.: Digitalisierung der Schweizer Demokratie. Technologische Revolution trifft auf traditionelles Meinungsbildungssystem, Zürich, 2021

[27] Humprecht, Edda, et. al.: Resilience to online disinformation: A framework for cross-national comparative research. In: International Journal of Press/Politics, Vol. 25, 2020, S. 493-516

[28] Staatsschreiberkonferenz SSK

[29] Etwa das seit 2012 jährlich von der BK organisierte Wahl- und Abstimmungsleitertreffen von Bund und Kantonen

[30] Vgl. u. a. Elections in times of crisis: Conference of the Council of Europe in Bern, https://www.parlament.ch/en/services/suche-news/elections-in-times-of-crisis> (aufgerufen am 27. Februar 2024) / Conférence parlementaire – Les élections en temps de crise (Berne, 9 et 10 mai 2023) <https://pace.coe.int/fr/pages/bern-elections-conference (aufgerufen am 27. Februar 2024)

[31] Jan Fivaz, Daniel Schwarz, Die Medienkompetenz der Schweizer Bevölkerung. Eine repräsentative Pilotstudie für die deutsch- und französischsprachige Schweiz, 2022, S. 15, 49-51, <https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/elektronische_medien/Zahlen%20und%20Fakten/Studien/schlussbericht-die-edienkompetenz-derschweizer-bevoelkerung.pdf.download.pdf/Bericht%20Medienkompetenz%202022%202.pdf>_(aufgerufen am 4. März 2024).

[32] Ibid., S. 6, 19-20.

[33] Bundesamt für Statistik, Omnibus 2021: Erhebung zur Internetnutzung, Steckbrief. <https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/erhebungen/omn2021.assetdetail.22284438.html> (aufgerufen am 4. März 2024)

Schweizer Bevölkerung im internationalen Vergleich im oberen Drittel: Fast 78 % der Bevölkerung nennen Grundkenntnisse oder höhere Kenntnisse.[34] Damit zeigt sich bezüglich Medienkompetenz eine Diskrepanz zwischen Selbsteinschätzung und tatsächlich gemessenem Kompetenzniveau.

Die Anzahl Personen in der Schweiz, die keine herkömmlichen Nachrichtensendungen konsumieren, nimmt zu.[35] Nur 22 % der 18- bis 24-Jährigen gaben im Jahr 2023 an, sich direkt von der Webseite oder der App eines Zeitungsverlags zu informieren, während es 2015 noch 53 % waren. Der Rest kommt über soziale Netzwerke mit Informationen in Berührung; bei den 15-29-Jährigen 40 % hauptsächlich über soziale und 25 % über Onlinemedien.[36] Soziale Medien sind kaum und Onlinemedien meist weniger als traditionelle Medien redaktionell moderiert. Viele Nutzende von sozialen Medien können leicht falsche für akkurate Informationen halten. Hinzu kommen gewisse Affinitäten gegenüber Verschwörungsnarrativen und Ideologien, die dazu beitragen können, dass Nutzerinnen und Nutzer Desinformationsinhalte, die zu bereits gehegten Überzeugungen passen, als wahr empfinden und weiterverbreiten.[37] Technologische Entwicklungen – namentlich KI – machen zudem das Erkennen von Desinformation zunehmend schwieriger (siehe 2.2). Eine andere Studie stellt fest, dass die Praxis der Überprüfung von Falschinformationen in der Gesellschaft relativ gut etabliert ist, insbesondere die Konsultation zusätzlicher Quellen oder die Überprüfung des Absenders, unter ihnen Informationen von Staat und Behörden (68 %), Medien-Webseiten (61 %), aber auch Google (45 %) und Austausch mit Verwandten (43 %).[38] Dedizierte Seiten zum Faktencheck sind im Schweizer Kontext kaum etabliert.

Zum Vertrauen in Medien attestiert die Eurobarometer-Umfragen der Schweiz leicht überdurchschnittliche Werte; für das Frühjahr 2023 wurde festgestellt, dass 53 % der Bevölkerung den Medien vertrauen (unverändert gegenüber 2021 und über dem EU-Durchschnitt von 36 %).[39] Klassischen Medien (72-82 %) wird weitaus stärker vertraut als Internetquellen (29 %) und insbesondere digitalen Plattformen (10 %).[40] Eine Studie weist darauf hin, dass dieses Vertrauen ein Stück weit erodiert und das allgemeine Vertrauen in die Schweizer Medien von 50 % im Jahr 2016 auf 42 % im Jahr 2023 gesunken ist.[41]

4.4 Ausblick

Angesichts machtpolitischer internationaler Entwicklungen ist es sehr wahrscheinlich, dass bestimmte staatliche oder staatlich beauftragte Akteure in den nächsten Jahren zunehmend Beeinflussungsaktivitäten und Desinformation einsetzen werden, um westliche Gesellschaften zu destabilisieren versuchen, und dabei neueste technologische Mittel nutzen. Diese Aktivitäten werden auch auf die Schweiz zielen. Die Schweiz ist durch ihre Kleinräumigkeit, regelmässige demokratische Partizipation, den hohen Bildungsgrad und das Vertrauen in die politischen Institutionen und Medien institutionell relativ robust gegen die Bedrohung. Dennoch – wie Befragungen zur Medien- und Informationskompetenz zeigen – erhöhen auch für die Schweiz die gewandelte Mediennutzung und technologischen Entwicklungen die Herausforderungen im Umgang mit Beeinflussungsaktivitäten und Desinformation.

---

[34] Vgl. Bundesamt für Statistik, Allgemeine digitale Kompetenzen der Bevölkerung im internationalen Vergleich, 2021 <https://www.bfs.admin.ch/asset/de/22404704> (aufgerufen am 4. März 2024).
[35] Forschungszentrum Öffentlichkeit und Gesellschaft der Universität Zürich, Jahrbuch Qualität der Medien 2022, <http://www.foeg.uzh.ch> (aufgerufen am 27. Februar 2024)
[36] Gemeinsam mit der Universität Oxford veröffentlichten Reuters-Studie 2023 zum Medienwandel; Stefan Thommen et al., Medienmonitor Schweiz 2022, Untersuchung der Publicom, S.50-52, <https://www.medienmonitor-schweiz.ch/uploads/media/default/0001/02/MMS_2022_Jahresbericht.pdf> (aufgerufen am 27. Februar 2024).
[37] Forschungszentrum Öffentlichkeit und Gesellschaft der Universität Zürich, Falschinformationen, Alternativmedien und Verschwörungstheorien – Wie die Schweizer Bevölkerung mit Desinformation umgeht, 2021, <https://www.foeg.uzh.ch/dam/jcr:96eb88c7-f0a2-4fc8-8fc2-6591e39195fa/Studie_01_2021.pdf> (aufgerufen am 27. Februar 2024)
[38] Vogler et al., Falschinformationen, Alternativmedien und Verschwörungstheorien, S. 31.
[39] Europäische Kommission, Standard-Eurobarometer, Die öffentliche Meinung in der Europäischen Union, Mai/Juni 2023, S. 74, <https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=88065> (aufgerufen am 4. März 2024)
[40] Europäische Kommission, Standard-Eurobarometer, Die öffentliche Meinung in der Europäischen Union, Januar/Februar 2022, S. 46ff. <https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=81061> (aufgerufen am 4. März 2024).
[41] Nic Newman et al., Reuters Institute Digital News Report 2023, S. 103, <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf> (aufgerufen am 5. März 2024)

KI ermöglicht einer noch breiteren Palette von Akteuren niederschwellig und mit noch weniger Aufwand ausgeklügelte Desinformation zu erstellen und zu verbreiten. Mit der fortschreitenden Entwicklung und Perfektionierung von KI zugrundeliegenden Algorithmen in den nächsten Jahren dürften diese zudem noch besser auf das Zielpublikum zugeschnitten sein und glaubwürdiger ausfallen und damit eine noch grössere Wirkung entfalten. KI bietet aber auch Chancen für Regulation, Faktencheck und das Aufdecken von Beeinflussungsaktivitäten und Desinformation. Diese Entwicklungen sind stark von grossen Technologieunternehmen geprägt, welche neue Technologien einführen und selbst Initiativen zur Selbstregulierung verfolgen. Auch die Bemühungen für Regulierung grosser Staaten oder von Wirtschaftsräumen, beispielsweise der USA und der EU, dürften sich intensivieren und Auswirkungen auf die Schweiz haben und der Schweiz Möglichkeiten der Übernahme bieten oder als Vorbild dienen.

5. Rechtliche Grundlagen in der Schweiz

Die relevanten Bestimmungen für den Umgang mit Beeinflussungsaktivitäten sind in verschiedenen Rechtstexten enthalten, insbesondere zu politischen Rechten und Medien, im Nachrichtendienstgesetz, zu sicherheitspolitischen Gremien, im Strafrecht und zu polizeilichen Aufgaben.

Die verfassungsmässige Garantie der politischen Rechte schützt die freie Willensbildung (vgl. Art. 34 Absatz 2 Bundesverfassung [BV; SR 101]). Die Verbreitung von Falschinformationen fällt grundsätzlich unter den Schutz der Meinungsfreiheit im Sinne von Art. 16 BV und Art. 10 EMRK und, je nach Konstellation, der Medienfreiheit im Sinne von Art. 17 BV. Das Bundesgericht vertritt in seiner Rechtsprechung die Grundannahme, dass die Individuen jede Meinung und Information sollen hören können, um sich im freien Austausch aller Äusserungen selbst eine Meinung bilden zu können.[42] Die Robustheit des institutionellen Informationssystems ist entscheidend, um möglichen Beeinflussungsaktivitäten und Desinformationen vorzubeugen und sie einzudämmen. Die Informationspolitik des Bundesrates basiert insbesondere auf Art. 180 der Bundesverfassung, Art. 10 des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG), Art. 10a des Bundesgesetzes über die politischen Rechte und den Richtlinien der Konferenz der Informationsdienste des Bundes (KID).

Die Meinungs*äusserung* darf nach den allgemeinen Regeln von Art. 36 BV (gesetzliche Grundlage, öffentliches Interesse oder Schutz von Grundrechten Dritter und Verhältnismässigkeit) eingeschränkt werden, etwa wo Persönlichkeitsrechte in Form übler Nachrede oder Verleumdung verletzt werden. Gesetzlich abgestützte Einschränkungen von Desinformation bestehen auch dort, wo der Schutz der öffentlichen Sicherheit und Ordnung tangiert ist.[43] Gewisse Handlungen im Informationsraum können zudem als Angriff auf die verfassungsmässige Ordnung strafbar sein (Art. 275 StGB).

Spezielle Regeln gelten für besonders sensible Bereiche der Meinungsbildung wie Informationssendungen in Radio und Fernsehen, wo für redaktionelle Sendungen mit Informationsgehalt das sogenannte «Sachgerechtigkeitsgebot» (Art. 4 Abs. 2 Bundesgesetz über Radio und Fernsehen [RTVG; SR 748.40]) besteht. Es ist verletzt, wenn Informationsinhalte so manipuliert werden, dass sich das Publikum kein persönliches Bild mehr machen kann. Dazu kann von jeder Person die Ombudsstelle von Radio und Fernsehen angerufen und nach deren Bericht Beschwerde an die unabhängige Beschwerdeinstanz für Radio und Fernsehen (UBI) erhoben werden (Art. 91-98 RTVG). Die Aufsicht über Werbeinhalte obliegt wiederum dem BAKOM. Generell dürfen Radio- und Fernsehsendungen nach Art. 4 Abs. 3 RTVG nicht die innere oder äussere Sicherheit des Bundes oder der Kantone und ihre verfassungsmässige Ordnung gefährden. Diese Bestimmung ist auch auf Werbung anwendbar; konkrete Anwendungsfälle existieren

---

[42] Vgl. etwa BGE 135 I 292, E. 4.1, S. 296. In seiner Rechtsprechung zu Art. 261*bis* StGB hielt das Bundesgericht zudem fest: «[I]n öffentlichen Debatten ist es oft nicht von Anfang an möglich, eindeutig zwischen unwahrer, halbwahrer und begründeter Kritik zu unterscheiden» (BGE 131 IV 23, E. 3.1, S. 28); Schefer Markus, Kommunikationsgrundrechte, in: Diggelmann Oliver et al. (Hrsg.), Verfassungsrecht der Schweiz, Band II, 2020, S. 1413-1452, Rz. 89; Raphaela Cueni, Falsche und irreführende Informationen im Verfassungsrecht der Schweiz, ex/ante 1/2019, 3, S. 12.

[43] Vgl. BGer 1P.336/2005 (20. September 2005), E. 5.3; EGMR, Mouvement raëlien suisse v. Switzerland (13. Juli 2012), 16354/06.

bisher jedoch nicht.[44] Gesetzliche Regelungen speziell für Intermediäre bestehen in der Schweiz noch nicht, sind aber in Ausarbeitung.

Die Regelungen des Nachrichtendienstgesetzes (NDG) sind auf die Zuständigkeiten des Nachrichtendiensts des Bundes (NDB) zum Thema Beeinflussungsaktivitäten anwendbar. So kann der NDB Beeinflussungsaktivitäten im Ausland bearbeiten, wenn diese für die sicherheitspolitische Lage der Schweiz von Bedeutung sind. Im Inland ist die Bearbeitung stärker eingeschränkt und nur zulässig, wenn ein relevanter Bezug zu Terrorismus, verbotenem Nachrichtendienst, Proliferation, Angriffen auf kritische Infrastrukturen oder gewalttätigem Extremismus besteht (Art. 6 Abs. 1 Bst. a Ziff. 1-5 NDG). Informationen über die politische Betätigung und über die Ausübung der Meinungs-, Versammlungs- und Vereinigungsfreiheit in der Schweiz darf der NDB grundsätzlich nicht bearbeiten (Art. 5 Abs. 5 NDG).

Beeinflussungsaktivitäten und Desinformation können je nach Ausprägung polizeiliche Aufgaben betreffen und es können – je nach Delikt – die Kantone oder der Bund Strafverfahren eröffnen. Relevant können die Verbrechen und Vergehen gegen den öffentlichen Frieden (Art. 258 ff StGB) sein, insbesondere die Schreckung der Bevölkerung (Art. 258 StGB). In Betracht gezogen werden müssen zudem der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB) sowie Diskriminierung und Aufruf zu Hass (Art. 261bis StGB).

Die Bundespolizei fedpol kann präventiv-polizeilich Material einziehen, das Propagandazwecken dienen kann und dessen Inhalt konkret und ernsthaft zur Gewalttätigkeit gegen Menschen oder Sachen aufruft. Liegt ein Verdacht auf eine strafbare Handlung vor, so übermittelt die sicherstellende Behörde das Material der zuständigen Strafbehörde (Art. 13e BWIS). Bei der Verbreitung von Gewaltpropaganda über das Internet kann fedpol nach Anhörung des NDB die Löschung der betreffenden Website auf einem schweizerischen Rechner verfügen oder dem schweizerischen Provider empfehlen, eine ausländische Webseite zu sperren. Falls Beeinflussungs- und Desinformationsaktivitäten von kriminellen Organisationen ausgehen, kann fedpol gestützt auf das ZentG[45] in eigener Kompetenz polizeiliche Vorermittlungen durchführen und dazu interkantonale und internationale Ermittlungsverfahren koordinieren. Dies kann beispielsweise relevant sein, weil staatliche russische Akteure nachweislich kriminelle Organisationen für ihre Zwecke einspannen.

fedpol kann gegenüber Ausländerinnen und Ausländern Einreiseverbote und Ausweisungen verfügen, wenn eine Person mit ihren Beeinflussungsaktivitäten die innere oder die äussere Sicherheit der Schweiz gefährdet (Art. 67 Abs. 4 und Art. 68 AIG). Ferner ergreift fedpol Schutzmassnahmen, wenn Desinformation zu einer Gefährdung von Schutzpersonen des Bundes (z. B. Bundesrätinnen und Bundesräte) und/oder zu einem erhöhten Schutzbedarf von Bundesgebäuden führt. Im Fall der gefälschten Energieplakate (siehe 4.2) eröffnete fedpol eine Untersuchung wegen Angriffs auf schweizerische Hoheitszeichen (Art. 270 StGB).

Weitere im vorliegenden Zusammenhang relevante Delikte mit Bundeskompetenz sind: Angriffe auf die Unabhängigkeit der Eidgenossenschaft (Art. 266 StGB), gegen die Sicherheit der Schweiz gerichtete ausländische Unternehmungen und Bestrebungen (Art. 266bis StGB), verbotene Handlungen für einen fremden Staat (Art. 271 StGB), verbotener Nachrichtendienst (Art. 272 ff. StGB), Vergehen gegen Volkswillen (Art. 279 ff. StGB; Art. 23 Abs. 1 Bst. h StPO) und Gewalt und Drohung gegen Behörden und Beamte (Art. 285 StGB).

6. Zuständigkeiten und bisherige Massnahmen in der Schweiz

Im Sicherheitspolitischen Bericht von 2021 hielt der Bundesrat fest, dass das Risiko von Beeinflussungsaktivitäten und Desinformation gegen die Schweiz steigt. Bei ihrer Bekämpfung sind die Stärkung der

---

[44] Im Rahmen seiner Aufsichtstätigkeit könnte des BAKOM gegen einen Programmveranstalter vorgehen, der in seiner Werbung Desinformation verbreitet und damit die innere oder äussere Sicherheit des Bundes oder der Kantone gefährdet. Das Aufsichtsverfahren kann sich dabei leidglich gegen schweizerische Veranstalter richten mittels die in Art. 89 Abs. 1 RTVG dargestellten Massnahmen. Ab wann eine effektive Gefährdung vorliegt, wäre anhand der konkreten Umstände einzuschätzen; mit Rücksicht auf die Programmautonomie ist eine solche Gefährdung indes nicht leichthin anzunehmen.

[45] Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten; SR 360c.

Lagebeobachtung und Früherkennung (6.1), die Stärkung der Resilienz der Schweiz und ihrer Bevölkerung im Sinne der Prävention (6.2), Regulierung und Sanktionen (6.3), Kommunikation und Zugang zu Behördeninformationen (6.4) und der Austausch unter den Behörden und die interne und externe Kooperation (6.5) zu nennen.

6.1 Lagebeobachtung und Früherkennung

Zurzeit existieren in der Schweiz keine Strukturen mit dem Ziel, umfassend systematische Beeinflussung im Informationsraum zu erkennen, ihre Absicht und Urheberschaft zu ermitteln und gegebenenfalls darauf zu reagieren.

Die sicherheitspolitischen Koordinationsorgane des Bundes, namentlich die Kerngruppe Sicherheit (KGSi) und der Sicherheitsausschuss des Bundesrats (SiA) mit Vorsitz VBS, haben die Aufgabe, die sicherheitspolitische Lage zu beurteilen und departementsübergreifende sicherheitspolitische Geschäfte zu koordinieren[46] und haben sich mehrfach mit Aspekten der Thematik befasst. Die KGSi kann basierend auf ihren Beratungen dem SiA Anträge unterbreiten.

Der NDB kann im Inland Informationen über Beeinflussungsaktivitäten nur sehr eingeschränkt sammeln, sichten oder verarbeiten. Er bearbeitet sicherheitspolitisch bedeutsame Beeinflussungsaktivitäten im Ausland und konzentriert sich dabei auf die direkte konkrete oder potenzielle Bedrohung der Schweiz durch die intensivierten Grossmächterivalitäten. Der NDB klärt die mit der hybriden Konfliktführung einhergehenden Beeinflussungsaktivitäten insbesondere Russlands und Chinas auf. Diese Aufklärung umfasst Akteure und Tätigkeiten im Ausland, welche die unbeeinflusste politische Willensbildung in der Schweiz oder in deren strategischem Umfeld untergraben, sowie Akteure und Tätigkeiten in der Schweiz, wenn ein relevanter Bezug zu Terrorismus, verbotenem Nachrichtendienst, Profileration, Angriffen auf kritische Infrastrukturen oder gewalttätigem Extremismus besteht.

Ein Medienmonitoring wird allgemein und permanent von den Departementen, den Bundesämtern und der Bundeskanzlei durchgeführt. Präsenz Schweiz des EDA beobachtet die Medienberichterstattung im Ausland zur Schweiz und wertet diese regelmässig aus. Die Bundeskanzlei und die Kantone nehmen mit Blick auf den Einsatz des elektronischen Stimmkanals bei eidgenössischen Urnengängen Risikobeurteilungen vor. Diese umfassen auch mögliche Angriffe durch Desinformation.

Das BAKOM wacht über das RTVG, seine Ausführungsbestimmungen und die Einhaltung der Konzessionen und überprüft die Erfüllung der Leistungsaufträge der SRG wie auch der privaten Veranstalter im Bereich des publizistischen Angebots u. a. mittels quantitativer Programmanalysen, die von Forschungsinstituten periodisch durchgeführt werden. Themen- oder amtsspezifischere Medienmonitorings führen in unterschiedlichem Ausmass auch die meisten anderen Departemente, Bundesämter und die Bundeskanzlei durch.

Ein Lagebild zu Beeinflussungsaktivitäten umfasst auch das Verfolgen entsprechender technologischer Entwicklungen. armasuisse Wissenschaft und Technologie und der Cyber-Defence-Campus arbeiten an verschiedenen Forschungsprojekten zu technologischen Aspekten im Zusammenhang von Beeinflussungsaktivitäten und Cyberabwehr, in Zusammenarbeit mit Schweizer Hochschulen. Als Beispiel wurde in einem Forschungsprojekt mit der Fachhochschule Nordwestschweiz (FHNW) das Bedrohungspotenzial durch KI-generierte Bilddaten analysiert. Die Forschung im Bereich der Datenwissenschaften (*Data Science*) trägt wesentlich zur Erkennung von Einflussblasen und zur Plausibilisierung von Trends in sozialen Netzwerken bei. Sie wird derzeit vom Cyber-Defence-Campus durchgeführt, ist aber durch den rechtlichen Rahmen von armasuisse Wissenschaft und Technologie teilweise eingeschränkt. Etwa dürfen Daten aus den sozialen Medien nicht anonymisiert werden, um diese in Forschungsarbeiten einzusetzen.

Desinformation kann Armeeangehörige bereits vor dem Eintritt in den Dienst oder während ihrer Auftragserfüllung beeinflussen. Die Armee beobachtet den Informationsraum deshalb im Alltag, insbesondere aber im Rahmen von Einsätzen und Operationen, Früherkennung von Aktionen gegen Angehörige

---

[46] Gemäss Weisungen des Bundesrats vom 25. Januar 2023, basierend auf Art 30 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit. Im SiA vertreten sind derzeit die Vorsteherin oder der Vorsteher des VBS, des EJPD und des EDA, begleitet von den Generalsekretärinnen oder Generalsekretären, den Staatsekretärinnen oder -sekretären EDA und SEPOS, den Direktorinnen und Direktoren von NDB und fedpol, und die Vizekanzlerin oder der Vizekanzler.

oder Basisleistungen der Armee. Entsprechende Erkenntnisse fliessen in einen wöchentlichen Lagerapport des Kommandos Operationen ein. Der Bereich CyMon (*Cyber-Monitoring*), eine Einheit des Kommando Cyber der Armee, analysiert Informationen von Webseiten und den sozialen Medien. CyMon nimmt dabei eine Vorauswertung der entsprechenden Daten vor und liefert Beiträge zur Detektion von Beeinflussungsaktivitäten gegen die Schweiz ohne Schweizer Beteiligung. Dies kann zugunsten der Armee und des militärischen Nachrichtendiensts im Rahmen des Militärgesetzes erfolgen, wenn diese Informationen armeerelevant sind, oder zugunsten des NDB auf dessen Auftrag hin und auf Basis des NDG.

Die Bundesverwaltung arbeitet mit Dritten wie der Forschung für ein besseres Bild der Betroffenheit der Schweiz. Ein vom BAKOM in Auftrag gegebener Bericht der Universität Zürich über Desinformation in der Schweiz (2021)[47], stellt die bislang umfassendste Studie zum Thema Desinformation dar. Das BAKOM hat die bestehende Literatur zu Desinformation zusammengetragen und damit begonnen, Desinformation in der Schweiz wissenschaftlich erforschen zu lassen mit Fokus auf Desinformationsinhalte, Rezeptionsverhalten, Charakteristika des Publikums und Gouvernanzansätze. Beeinflussungsaktivitäten fallen unter diese Forschung, die jedoch breiter angelegt ist und nicht speziell auf staatliche Desinformation fokussiert.[48]

6.2 Resilienz durch Sensibilisierung, Bildung und Medienkompetenz

Resilienz und Prävention umfassen die Sensibilisierung für das Phänomen, seine Ausprägung, mögliche Konsequenzen und die Betroffenheit der Schweiz. Zielgruppen entsprechender Aktivitäten sind das Bundespersonal (einschliesslich Vertretungen im Ausland), kantonale Behörden, die Öffentlichkeit, politische Akteure (z. B. Parteien) und Medienschaffende.

Konkret übten Beteiligte des Bundes und der Kantone die Reaktion auf Beeinflussungsaktivitäten und Desinformation bei einem Krisenereignis im Rahmen der grossangelegten Sicherheitsverbundsübung 2019, welche damit für die Thematik sensibilisiert. Zum Gesamtthema Terrorbedrohung wurde simuliert, wie mit politischen Drohungen, Propaganda und Desinformation Unsicherheit bei den Behörden und der Bevölkerung geschürt würde, einschliesslich mittels Cyberangriffen auf Informationsportale von Bund und Kantonen und durch gezielte Manipulation der Medien. Dies geschah zwar durch eine fiktive terroristische Gruppe, doch bei entsprechendem Vorgehen staatlicher Akteure im Informationsraum dürften sich ähnliche Herausforderungen stellen.

Mit Blick auf die Nationalratswahlen 2019 und 2023 hat die Bundeskanzlei die Parteien, die grossen Plattformen, das NCSC/BACS sowie den Eidgenössischen Datenschutzbeauftragten zu einem Treffen zu «Kampagnen im digitalen Raum» eingeladen. Ziele waren die Sensibilisierung für die Bedrohung durch Beeinflussungsaktivitäten und die Diskussion möglicher Schutzmassnahmen. Ausserdem wurden mit Google, Meta und Tiktok privilegierte Zugänge im Vorfeld der Nationalratswahlen vereinbart, welche Direktkontakte bei allfälligen Manipulationen vorsahen und dass behördliche Informationen auf diesen Plattformen privilegiert angezeigt wurden.

Qualitätsmedien mit hohen journalistischen Standards und ein interessiertes, kritisches Publikum, wie es in der Schweiz grundsätzlich zutrifft, tragen zur Eindämmung der Wirkung von Beeinflussungsaktivitäten bei. Der Bundesrat hat in Erfüllung des Postulats Christ 21.3781 «Strategie für eine zukunftsgerichtete Medienförderung jetzt aufgleisen» in einem Bericht unterschiedliche Finanzierungmöglichkeiten und -modelle zur Medienförderung dargelegt, die kanalunabhängig umgesetzt werden können. Im Bereich der Förderung der journalistischen Aus- und Weiterbildung arbeitet das BAKOM zurzeit an der Umsetzung der parlamentarischen Initiative Chassot 22.417 zu Fördermassnahmen für Institutionen, die Aus- und Weiterbildungen für redaktionell tätige Mitarbeitende von elektronischen Medien anbieten. Zudem hat das BAKOM 2023 einen Nationalen Aktionsplan für die Sicherheit von Medienschaffenden[49]

---

[47] Vogler et al., Falschinformationen, Alternativmedien und Verschwörungstheorien.
[48] Für einige Erkenntnisse aus diesen Studien, siehe 3.1 und 3.3.
[49] <https://www.bakom.admin.ch/bakom/de/home/elektronische-medien/medienpolitik/nationaleraktionsplan.html#:~:text=Der%20Nationale%20Aktionsplan%20f%C3%BCr%20die,Medienschaffenden%20in%20der%20Schweiz%20dar>

verabschiedet. Insbesondere sollen Medienschaffende besser vor Drohungen, Gewalt und Einschüchterungsversuchen geschützt werden, welche alle auch durch Beeinflussungsaktivitäten begünstigt werden dürften.

Ein zentrales Element der Resilienz und der Prävention gegenüber Beeinflussungsaktivitäten und Desinformation ist Bildung. Elemente dazu setzen auf allen Bildungsebenen bei Kindern, Jugendlichen und Erwachsenen an. Ältere Erwachsene sind durch Bemühungen im Bereich Bildung sehr viel schwieriger zu erreichen. Die Lehrpläne der obligatorischen Schule, die in die Zuständigkeit der Kantone fällt, sehen politische und digitale Bildung vor.[50] Das Ziel ist, junge Menschen dazu zu befähigen, sich über das politische und soziale Leben zu informieren und daran teilzunehmen. Konkret vermitteln die sprachregionalen Lehrpläne Sach-, Urteils-, Handlungs- und Methodenkompetenz, um kritisch und verantwortungsbewusst mit Medien und Informationen umzugehen. Auch in den revidierten Rahmenlehrplänen für den allgemeinbildenden Unterricht der beruflichen Grundbildung und für die Berufsmaturität wird die Thematik des kritischen Umgangs mit Medien und Informationen verstärkt. Ebenso leisten die Berufsbildungsverantwortlichen einen Beitrag zur Förderung digitaler Kompetenzen.[51] Nach einem Beschluss des Bundesrates und der EDK aus dem Jahr 2018 belegen spätestens seit dem Schuljahr 2022/2023 schweizweit alle Schülerinnen und Schüler an Gymnasien obligatorisch Informatik. Auf Hochschulebene wird der Bund voraussichtlich 2025 bis 2028 projektgebunden das zukünftige Programm *Open Education & Digital Competencies* fördern. Dabei sollen die Lehrkräfte bei der Entwicklung einer digitalen Kultur im Unterricht mit Schwerpunkt auf der Qualität der digitalen Medien sowie die Kompetenzen der Studierenden, digitale Daten zu bewerten und sich den Herausforderungen der KI zu stellen, unterstützt werde.

Medienverbände, beispielsweise der Verband Schweizer Medien, tragen mit Projekten zu (digitaler) Medienkompetenz von Jugendlichen bei.[52] Das Portal ch.ch, die gemeinsame Informationsplattform von Bund, Kantonen und Gemeinden zum Leben in der Schweiz, erklärt, wie die Bevölkerung Desinformation erkennen und damit umgehen kann. Das Bundesamt für Sozialversicherungen betreibt indes die nationale Plattform Jugend und Medien zur Förderung von Medienkompetenz.

6.3 Regulierung und Sanktionen

Das BAKOM veröffentlichte unter Mitarbeit der Bundeskanzlei 2021 den Bericht «Intermediäre und Kommunikationsplattformen: Auswirkungen auf die öffentliche Kommunikation und Ansätze einer Governance», der positive und negative gesellschaftliche Potenziale digitaler Plattformen aufzeigt und die bestehenden Regulierungsansätze in Europa diskutiert.[53] Am 5. April 2023 hat der Bundesrat das UVEK (BAKOM) beauftragt, eine Vernehmlassungsvorlage zur Regulierung von Kommunikationsplattformen auszuarbeiten. Diese wird sich auch mit den Herausforderungen befassen, die sich aus der mangelnden Rechtsdurchsetzung gegenüber den digitalen Plattformen ergeben. Sie orientiert sich am *Digital Services Act* der EU und hat zum Ziel, insbesondere sehr grosse Plattformen anhand von Sorgfalts- und Berichterstattungspflichten stärker in die Verantwortung zu nehmen. Allerdings wird Desinformation nur dort von der Regulierung tangiert, wo es sich um rechtswidrige Inhalte handelt.

Im Bereich Sanktionen hat die Schweiz namentlich diejenigen der EU vom 1. März 2022 gegen RT und Sputnik – wichtige staatsnahe russische Nachrichtenportale im Ausland – nicht übernommen. Auch

[50] Eidgenössisches Departement für Wirtschaft, Bildung und Forschung (WBF), Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren (EDK), Chancen optimal nutzen. Erklärung 2023 zu den gemeinsamen bildungspolitischen Zielen für den Bildungsraum Schweiz, 26. Oktober 2023, <https://www.sbfi.admin.ch/dam/sbfi/de/dokumente/2023/10/erklaerung-chancen-2023.pdf.download.pdf/erklaerung-chancen-2023_d.pdf> (aufgerufen am 5. März 2023)
[51] gemäss revidierten Rahmenlehrplänen für Berufsbildungsverantwortliche
[52] Vgl. das Dossier «Medienkompetenz» das Verlegerverbands Schweizer Medien, <https://www.schweizermedien.ch/medienkompetenz>
[53] Bundesamt für Kommunikation, Intermediäre und Kommunikationsplattformen: Auswirkungen auf die öffentliche Kommunikation und Ansätze einer Governance, 17. November 2021, <https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/elektronische_medien/Zahlen%20und%20Fakten/Studien/bericht-kommunikationsplattformen-und-intermediaere-2021.pdf.download.pdf/Bericht%20Kommunikationsplattformen%20und%20Intermedi%C3%A4re.pdf> (aufgerufen am 5. März 2024)

wenn es sich bei diesen Kanälen um Werkzeuge der gezielten russischen Propaganda und Desinformation handelt, ist der Bundesrat der Meinung, dass es wirksamer sei, unwahren und schädlichen Äusserungen mit Fakten zu begegnen, anstatt sie zu verbieten. Die Reichweite dieser Medien in der Schweiz gilt als gering.

6.4 Kommunikation

Zu unterscheiden sind Kommunikationsmittel zur Bewältigung von und Reaktion auf Beeinflussungsaktivitäten und Desinformation einerseits sowie Kommunikation zur regelmässigen Information der Bevölkerung und politischer Akteure im Sinne der Prävention andererseits.

Eine Beeinflussungsaktivität kann auch dann politisch unerwünscht sein, wenn sie nicht gegen geltendes Recht verstösst. Der Bundesrat und die Bundesverwaltung können falsche oder irreführende Informationen, die in der Öffentlichkeit verbreitet werden, korrigieren (*Debunking*), machen von dieser Möglichkeit aber nur zurückhaltend Gebrauch. Einerseits fällt die Verbreitung falscher Informationen unter das Recht auf freie Meinungsäusserung, sofern es sich nicht um strafrechtlich relevante Angriffe handelt. Mit dem Scheinwahrheitseffekt, wonach oftmals wiederholte – auch falsche – Aussagen für wahrer gehalten werden, kann Debunking die Wirkung von Desinformation sogar verstärken. Misstrauen und der Glaube an einen «wahren Kern» einer Falschinformation könnten gestärkt werden, wenn Richtigstellungen der Behörden als besonders offensiv und vehement wahrgenommen werden. Die Social-Media-Leitlinien der Konferenz der Informationsdienste des Bundes definieren die Kriterien für die Reaktion auf Desinformationen auf den neuen Informationsplattformen, «wenn sie sich über die Gemeinschaft, aus der sie stammen, oder über ihr nahe stehende Gemeinschaften hinaus verbreiten oder schädlich sind». Die Bundesverwaltung berichtigt grundsätzlich nur dann.[54] Das UVEK kommunizierte beispielsweise zur Verbreitung des falschen Energieplakats (siehe 4.2).

Im Gegensatz zu Debunking zeigen Forschungsergebnisse hingegen die hohe Relevanz von Sensibilisierungsmassnahmen und der Stärkung der Eigenverantwortung zur Prävention (*Prebunking*).[55] Unmittelbares Prebunking, welches über spezifische sich abzeichnende Beeinflussungsaktivitäten informiert und diese vorab entlarvt und/oder entkräftet, verfolgt der Bundesrat derzeit nicht und würde ein detailliertes Lagebild voraussetzen.

Der Bundesrat verfolgt aber allgemein eine direkte, umfassende, mehrsprachige, transparente und kontinuierliche Informationspolitik, die Beeinflussungsversuche erschwert. Informationen über die Geschäfte des Bundesrates, die Tätigkeit der Verwaltung und über Abstimmungen und Wahlen[56] werden in mehreren Sprachen und über mehrere Kanäle verbreitet, u.a. durch regelmässige Medienkonferenzen, an denen die Mitglieder des Bundesrates persönlich auftreten und Auskunft geben. Die Informationen des Bundesrates werden zunehmend mit Erklärungsvideos und Infografiken unterstützt. Die Anwendung VoteInfo, ein mit den Kantonen und Gemeinden entwickelter direkter Informationskanal, stellt der breiten Öffentlichkeit Informationen und Ergebnisse zu eidgenössischen und kantonalen Abstimmungen zur Verfügung. Die genannten Massnahmen im Bereich der Kommunikation dürften die Reichweite der Informationen bei gewissen Zielgruppen erhöhen, können aber nur begrenzt der Herausforderung von Beeinflussungsaktivitäten begegnen.

Derzeit konzipiert die Bundeskanzlei eine Informations-App für die Kommunikation des Bundesrates al direkten Kanal zur Bevölkerung. Gemäss einer Studie des Meinungsforschungsinstitut gfs.bern im Jahr 2022 finden 70 % der Befragten eine solche Informations-App interessant und 75 % den Ansatz sinnvoll. Dieser Kanal wäre von den grossen bestehenden Social-Media-Plattformen unabhängig und kann von möglichen Beeinflussungsaktivitäten abgeschirmt werden. Er könnte zudem sowohl im Krisenfall wie auch im Fall von Beeinflussungsaktivitäten, bei denen eine Reaktion seitens des Bundesrats erforderlich wäre, eingesetzt werden (Push-Benachrichtigung).

---

[54] Bundeskanzlei, Leitlinien für die Kommunikation in den Sozialen Medien, Mai 2021, Art. 7, <https://www.newsd.admin.ch/newsd/message/attachments/67321.pdf> (aufgerufen am 5. März 2024)
[55] Jon Roozenbek et al., A Practical Guide to Prebunking Misinformation, 2022, <https://interventions.withgoogle.com/static/pdf/A_Practical_Guide_to_Prebunking_Misinformation.pdf> (aufgerufen am 5. März 2024)
[56] Im Rahmen der rechtlichen Vorgaben; für eidgenössische Volksabstimmungen vgl. namentlich Art. 10*a* sowie Art. 11 Abs. 2 Bundesgesetz über die politischen Rechte (161.1; BPR) sowie für die Nationalratswahlen Art. 34 BPR.

Desinformation kann während bevölkerungsschutzrelevanten Krisen, etwa bei Stromausfällen, gravierende Folgen haben. Es kann die Kompetenz der staatlichen Institutionen, effektiv auf die Krise zu reagieren, erschüttern. Falsche Informationen etwa über die Ursachen eines Stromausfalls können Misstrauen schüren, sodass Bürgerinnen und Bürger den Anweisungen der Behörden, wie Evakuierungsbefehlen oder Sicherheitshinweisen, nicht folgen. Der App und der Website Alertswiss, die vom Bund und den Kantonen als Instrument zur Warnung, Alarmierung und Information der Bevölkerung bei der Bewältigung von Katastrophen und Notsituationen eingesetzt werden, kommt in diesem Zusammenhang eine Schlüsselrolle zu. Alertswiss kann als direkter Kommunikationskanal dienen, um die Bevölkerung über ereignisbezogene Notsituationen zu informieren und mittels genauer, zeitnaher und überprüfbarer Information die Verbreitung von Desinformation zu bekämpfen. Um die Effektivität von Alertswiss im Kontext von Desinformation zu optimieren, werden die Stakeholder (Nutzerinnen und Nutzer auf Stufe Bund und Kantonen) im Rahmen der Ausbildungen, in den Fachgremien und via die bestehenden Informationsplattformen vermehrt auf diesen Nutzen sensibilisiert.

Es ist bezüglich Kommunikation zu bemerken, dass im Falle eines bewaffneten Konflikts mit Beteiligung der Schweiz andere Massnahmen in Betracht gezogen werden müssten als in der normalen Lage. Die Schweizer Armee befasst sich deshalb mit dem Einsatz von Mitteln in allen Wirkungsräumen, einschliesslich dem Informationsraum im Konfliktfall, was im Rahmen dieses Berichts nicht vertieft wird. Als ein Instrument der Sicherheitspolitik muss die Armee im Falle eines bewaffneten Konflikts in der Lage sein, im Rahmen der strategischen Vorgaben des Bundes militärische Aktionen im Informationsraum selbstständig oder in Zusammenarbeit mit den zivilen Behörden zu führen.

6.5 Koordination und Austausch

Die Vielschichtigkeit und Breite des Themas erfordert engen Informationsaustausch und Koordination innerhalb der Bundesverwaltung, zwischen der Bundesverwaltung, Medien, Plattformen, der Forschung und mit internationalen Partnern und Institutionen.

Eine zentrale Koordination und umfassende Lageanalyse bestehen bislang nicht, denn die Kompetenzen sind verteilt. In den letzten Jahren wurden jedoch Ansätze zur Förderung der Koordination und des Austauschs verfolgt. Um die Betroffenheit festzustellen und Koordination innerhalb der Bundesverwaltung zum Thema zu fördern, haben die KGSi und die Bundeskanzlei im Januar 2021 eine Erhebung zum Thema in der Bundesverwaltung durchgeführt, um eine Übersicht über in der Bundesverwaltung laufende oder geplante Arbeiten rund um Beeinflussungsaktivitäten und Desinformation zu erhalten. Dazu identifizierte die KGSi Ansprechstellen für die Früherkennung und Bearbeitung von Beeinflussungsaktivitäten. Die Umfrage stellte potenzielle Betroffenheit bei fast allen Verwaltungseinheiten fest. Seit August 2022 besteht ein Netzwerk von Kontaktpersonen in Departementen und Ämtern zu Beeinflussungsaktivitäten und das EDA hat mehrere Workshops innerhalb der Bundesverwaltung zum Thema organisiert. Koordinations- und Diskussionsplattformen bestehen auch zwischen der Bundesverwaltung und externen Beteiligten sowie multilateral.

Die Schweiz tauscht sich auch mit Partnerstaaten und in multilateralen Foren über den Umgang mit Beeinflussungsaktivitäten und Desinformation aus. Sie erachtet diesen Austausch als wichtige Massnahme, da Beeinflussungsaktivitäten aufgrund ihrer transversalen Auswirkungen verschiedene Staaten betreffen und allfällige Reaktion und Lagebilder mittels internationaler Kooperation und Koordination gestärkt werden können. Da sie in verschiedenen Institutionen (Nato, EU, G7) nicht Mitglied ist, ist der Zugang der Schweiz zu Informationen nicht selbstverständlich, aber es gab verschiedene Expertentreffen mit der EU. Mit dem Vereinigten Königreich wurde 2023 eine engere Zusammenarbeit in diesem Bereich initiiert und ein jährlicher Austausch gepflegt.

Auf europäischer Ebene erarbeitet der Lenkungsausschuss für Medien und Informationsgesellschaft des Europarats (CDMSI) Massnahmen und Empfehlungen zur Bekämpfung von Falschinformationen. So veröffentlichte ein Expertenkomitee unter Schweizer Vorsitz beispielsweise Leitlinien zur menschenrechtskonformen Bekämpfung von Falsch- und Desinformationen durch Faktenüberprüfung und Vorgaben zur Ausgestaltung von Online-Plattformen.[57] 2020 veröffentlichte die *Freedom Online Coalition*, der die Schweiz ebenfalls angehört, eine gemeinsame Erklärung zu Desinformation. Ende August 2023 kündigte sie die Einrichtung einer Task Force zur Vertrauenswürdigkeit von Online-Informationen an. Das

---

[57] Europarat, Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner, März 2024, <https://rm.coe.int/cdmsi-2023-015-msi-inf-guidance-note/1680add25e> (aufgerufen am 5. April 2024).

BAKOM beteiligt sich an der Arbeit des Digital Policy Lab des *Institute for Strategic Dialogue*, das auf eine Initiative Deutschlands zurückgeht und eine Austauschplattform mit gleichgesinnten Staaten zu den Themen Desinformation, Hassrede und Plattformregulierung bietet. 2022 beteiligte sich das SEM im Rahmen intergouvernementaler Aktivitäten der Migrationsbehörden (IGC) an einer 10-Punkte-Toolbox zur Stärkung der Nato- und EU-Mechanismen, um hybriden Bedrohungen zu widerstehen, welche die Instrumentalisierung von Migrationsbewegungen, auch im Informationsraum, umfassen kann.

7. Weitere Massnahmen und Handlungsoptionen

Eine wirksame Bekämpfung von Beeinflussungsaktivitäten und Desinformation setzt einen gesamtgesellschaftlichen Ansatz voraus. Isolierte Massnahmen einer Behörde oder Institution werden angesichts des koordinierten Vorgehens und des Einsatzes von erheblichen Ressourcen staatlicher ausländischer Akteure sowie der technologischen Entwicklungen nicht genügen. Eine vollständige Eindämmung der Bedrohung ist in einer freien Gesellschaft und angesichts der Verbreitung neuer technologischer Mittel nicht möglich, doch verschiedene, bereits genannte Massnahmen sollen teilweise vertieft und durch weitere ergänzt werden, vor allem zur Lagebeobachtung, Früherkennung und Koordination.

Lagebeobachtung und Früherkennung

Künftig soll die Kerngruppe Sicherheit regelmässig die Thematik Beeinflussungsaktivitäten und Desinformation traktandieren, mindestens zwei Mal jährlich, und bei Bedarf den SiA und den Bundesrat damit befassen. Die in der KGSi und im SiA vertretenden Departemente – das VBS mit dem NDB und SEPOS; das EJPD mit fedpol; das EDA mit dem Staatssekretariat – können dem Bundesrat allfällige Massnahmen zum Entscheid vorlegen. Ferner soll geprüft werden, wie die künftige Analyse und Lagebeurteilung von Desinformation zu koordinieren ist mit dem Ziel, Beeinflussung im Informationsraum durch staatliche Akteure zu identifizieren, ihre Urheber und deren Absicht zu ermitteln und Massnahmen zu identifizieren. Die bestehen Arbeiten und Monitorings aller betroffenen Ämter sollen einfliessen und können ergänzt werden, um ein umfassenderes Lagebild zu erhalten und Information zu teilen. Ebenso soll das Potenzial zum Ausbau und zur Institutionalisierung des internationalen Austauschs und der Zusammenarbeit zum Lagebild geprüft werden, namentlich bezüglich Zugangs zu und Beteiligung an Datenbanken und Analysen des Europäischen Auswärtigen Diensts und dem Vereinigten Königreich zum multilateralen System. Ferner sollen mögliche Massnahmen geprüft werden wie ein zentrales und öffentliches Portal für Faktenchecks, bspw. durch die Förderung einer unabhängigen Aufsichtsstelle oder einem Forschungsinstitut.

Resilienz durch Sensibilisierung, Bildung und Medienkompetenz

Das Thema für die umfassende Integrierte Übung 2025 (IU 25), welche die Bundeskanzlei gemeinsam mit dem VBS und den Kantonen organisiert, wird eine hybride Bedrohung gegen die Schweiz sein. In diesem Übungskontext wird das Thema Beeinflussungsaktivitäten und Desinformation und der Umgang damit eine zentrale und wichtige Rolle spielen. Zudem soll in der Forschungsunterstützung, welche das BAKOM begonnen hat, im Rahmen eines Programms neu ein Schwerpunkt gebildet werden auf der Wirkung von Desinformation in kurz-, mittel- und langfristiger Perspektive, um Desinformation im Kontext der Meinungsbildung zu untersuchen. Ein besseres Verständnis für die Effekte von Desinformation im Schweizer Kontext dient der Lageeinschätzung und Bemühungen zu Sensibilisierung und Prävention.

Alle drei sprachregionalen Lehrpläne der obligatorischen Schule sowie die Rahmenlehrpläne der Sekundarstufe II beinhalten politische und digitale Bildung. Verschiedene Plattformen staatlicher Stellen informieren über Desinformation und bieten Lehrangebote zu Medien- und Politkompetenz. Angesichts des bereits sehr umfangreichen Angebots ist eine Ausweitung oder Vertiefung kurzfristig nicht erforderlich. Dank der hohen Flexibilität und der engen Zusammenarbeit der Bildungsakteure ergeben sich im Bedarfsfall rasche Handlungsmöglichkeiten.

Regulierung und Sanktionen

Das BAKOM arbeitet aktuell eine Vernehmlassungsvorlage zur Regulierung von sehr grossen Kommunikationsplattformen aus. Allfällige neue Sanktionen der EU gegen Nachrichtenportale, die Desinformation verbreiten, wird der Bundesrat unter Berücksichtigung der besonderen Umstände, der Verhältnismässigkeit und des aussen- und sicherheitspolitischen Nutzens abwägen.

Kommunikation

Der Bundesrat bzw. die Bundesverwaltung berichtigen Desinformation vor dem Hintergrund der Meinungsäusserungsfreiheit nur zurückhaltend und verfügen über eine entsprechende Leitlinie der Konferenz der Informationsdienste des Bundes.[58] An diesem Grundsatz wird festgehalten. Der Bundesrat kommuniziert weiterhin direkt, umfassend und transparent auf verschiedenen Kanälen, was Beeinflussungsaktivitäten erschwert. Die zusätzlichen Arbeiten und der Austausch im Rahmen der Analyse und des Lagebilds sollen in die Abwägungen des Bundes bezüglich Kommunikation von Vorfällen und allfälliger diplomatischer Massnahmen einfliessen.

Austausch und Koordination

In der Bundesverwaltung wird seit 2022 ein Netzwerk von Kontaktpersonen zu Beeinflussungsaktivitäten gepflegt und es werden regelmässig Workshops innerhalb der Bundesverwaltung zum Thema organisiert. Dieser Austausch dient dazu, ein gemeinsames Verständnis für diese sicherheitspolitische Bedrohung, relevante Entwicklungen, die Lage und die relevanten Aktivitäten beim Bund zu fördern und um Massnahmen abzuleiten und abzustimmen. Ferner werden in den Austausch Fachpersonen aus der Wissenschaft oder dem Ausland sowie Zuständige in anderen Staaten eingebunden. Die laufenden internationalen Austausche mit Partnerstaaten und in multilateralen Foren zum Austausch von Fachwissen und zur Stärkung des Lagebilds werden laufend gepflegt und sollen, wo sinnvoll, ausgebaut werden. Der Austausch innerhalb der Bundesverwaltung soll künftig ausgebaut und gegebenenfalls institutionalisiert werden. In diesem Rahmen sind auch Bezüge zu Arbeiten rund um transnationale Repression zu prüfen. Die Bedrohung durch Beeinflussungsaktivitäten und Desinformation und ihre sicherheitspolitische Bedeutung haben zugenommen, was den Koordinationsbedarf erhöht. Die Abstimmung mit den sicherheitspolitischen Gremien des Bundes ist zu verstärken und die künftig stärker koordinierte Analyse und Lagebeurteilung sollen sowohl in deren Erwägungen wie den Austausch in der Bundesverwaltung einfliessen.

[58] Bundeskanzlei, Leitlinien für die Kommunikation in den Sozialen Medien, Mai 2021, Art. 7, <https://www.newsd.admin.ch/newsd/message/attachments/67321.pdf> (aufgerufen am 5. März 2024).

8. Glossar

Beeinflussungsaktivitäten: Beeinflussungsaktivitäten im Informationsraum umfassen ein grösseres Instrumentarium, zu dem Desinformation zählt, und zielen darauf ab, die Wahrnehmung, das Denken und das Handeln von Individuen, Gruppen und Gesellschaften zu manipulieren. Diese Aktivitäten können von staatlichen oder nichtstaatlichen Akteuren betrieben werden (siehe 2.1).

Beeinflussungsoperation: Ein Beeinflussungsakteur kann mehrere Aktivitäten im Informationsraum im Rahmen einer Beeinflussungsoperation koordinieren.

Beeinflussungskampagne: Im Rahmen einer Beeinflussungskampagne koordiniert ein Beeinflussungsakteur, der über einen hohen Grad an Fähigkeiten und Ressourcen verfügt, Beeinflussungsoperationen. Die einzelnen der Kampagne zugrundeliegenden Aktivitäten können dabei auf verschiedenen Beeinflussungsmitteln basieren (z.B. Desinformation, Cyberangriffe oder Druckausübung).

Desinformation: irreführende oder vollständig erfundene Informationen, die absichtlich verwendet werden, um auf die Meinungsbildung der Bevölkerung Einfluss zu nehmen, politische Prozesse zu beeinflussen, die Glaubwürdigkeit von Institutionen und Medien anzugreifen oder Zweifel an der Zuverlässigkeit von Informationen zu säen (siehe 2.1).

Fake News: falsche Tatsachenbehauptungen, die in bösem Glauben geäussert und zu Zwecken der politischen Manipulation, aus finanziellen oder anderen persönlichen Gründen verbreitet werden und ihre Macht aus der neuen Dynamik der sozialen Netzwerke ziehen.[59]

Falschinformation/Fehlinformation: Falschinformation (englisch: *misinformation*) kann auch schlicht eine faktisch inkorrekte, fehlerhafte oder irreführend Information beschreiben, unabhängig von ihrer Verwendung und dem Bewusstsein des Akteurs, dass die Information falsch ist.

FIMI: Die EU benutzt den Begriff *Foreign Information Manipulation and Interference*, sinngemäss "ausländische Informationsmanipulation und Beeinflussung". Für die EU entspricht FIMI nicht-illegalen Verhaltensweisen, die politische Werte, Verfahren und Prozesse bedrohen oder sich negativ auf diese auswirken können. Es handelt sich um eine manipulative Aktivität, die absichtlich und mitbestimmungspflichtig durchgeführt wird. Die EU hat dazu ein standardisiertes Analyseraster ausgearbeitet.

Malinformation: wahre Information, die mit der Absicht verbreitet wird, Schaden zu verursachen; oftmals durch Leaks von nicht für die Öffentlichkeit bestimmten Informationen.

Misinformation: siehe «Falschinformation».

Propaganda: kann als Instrument zur Beeinflussung von Meinungen im Grundsatz der Wahrheit entsprechen; die Informationen werden jedoch bewusst so gewählt, gefärbt und ausgelegt, dass sie eine bestimmte Auffassung oder Sichtweise beim Empfänger erzeugen und fördern. Wenn als legitim geltende diplomatische Kanäle, beispielsweise das X/Twitter-Konto einer ausländischen Vertretung, Desinformation verbreitet, vermischen sich diese Kategorien. Propaganda ist ein Element von Beeinflussungsaktivitäten im Informationsraum und unterscheidet sich (teilweise) von Desinformation, indem sie auch wahr sein kann. Propaganda baut oft auf erwiesenen Fakten auf, diese werden aber ergänzt durch bewusst manipulierte, einseitig kontextualisierte oder dekontextualisierte Interpretationen.

---

[59] Bericht des Bundesrates, Rechtliche Basis für Social Media: Erneute Standortbestimmung. Nachfolgebericht des Bundesrates zum Postulatsbericht Amherd 11.3912 „Rechtliche Basis für Social Media“, Mai 2017, <https://www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/social_media/social%20media%20bericht.pdf.download.pdf/social-media-bericht-2017-DE.pdf> (aufgerufen am 5. März 2024)